2013-11-25

2013-11-25

Finansinspektionen
Box 7821
SE-103 97 Stockholm
[Brunnsgatan 3]
Tel +46 8 787 80 00
Fax +46 8 24 13 35
finansinspektionen@fi.se
www.fi.se

Enligt sändlista

FI Dnr 11-11528, 12-4167
(Anges alltid vid svar)

Remiss - förslag till nya regler om hantering av operativa risker samt nya regler om it-system, informationssäkerhet och insättningssystem i kreditinstitut och värdepappersbolag

Finansinspektionen föreslår två nya föreskrifter som innebär skärpta krav på banker, kreditmarknadsföretag och värdepappersbolag att hantera operativa risker i sin verksamhet på ett effektivt och sunt sätt. Syftet är att minska risken för händelser i företagens verksamhet som resulterar i höga förluster eller omfattande störningar, vilket i sin tur bidrar till att upprätthålla ett stabilt och väl fungerande finansiellt system.

De krav på hantering av operativa risker som finns i dag är få och generellt utformade. Finansinspektionen bedömer att det behövs mer precisa regler som ger företagen bättre förutsättningar att på ett strukturerat och systematiskt sätt identifiera, mäta och bedöma operativa risker.

De båda föreskrifterna och allmänna råden om dels hantering av operativa risker, dels it-system, informationssäkerhet och insättningssystem, innebär också att företagen ska tillsätta resurser och genomföra åtgärder för att hantera riskerna.

Utöver detta föreslås följdändringar i Finansinspektionens föreskrifter (FFFS 2007:16) om värdepappersrörelse.

Genom förslagen inför Finansinspektionen Baselkommitténs riktlinjer Principles for the sound management of operational risk och delar av Europeiska bankmyndighetens riktlinjer för intern styrning (GL 44) som bindande regler. Dessutom införs särskilda krav på företag som erbjuder tjänster som omfattas av den statliga insättningsgarantin. Dessa syftar till att slutligt anpassa den svenska regleringen till det så kallade insättningsgarantidirektivet.

De nya och ändrade reglerna föreslås träda i kraft den 1 maj 2014.

Finansinspektionen bifogar förslag till författningstexter en remisspromemoria samt en ändringsföreskrift till Finansinspektionens föreskrifter om värdepappersrörelse. Remissmaterialet finns också på vår webbplats, www.fi.se.

Skriftliga synpunkter på förslagen lämnas till Finansinspektionen, Box 7821, 103 97 Stockholm eller via e-post till finansinspektionen@fi.se senast den **10 januari 2014**.

Frågor om remissen avseende hantering av operativa risker besvaras av Agnieszka Arshamian (08-787 83 78 eller agnieszka.arshamian@fi.se) och avseende it-system, informationssäkerhet och insättningssystem av Anders Lindgren (08-787 81 38 eller anders.lindgren@fi.se).

Med vänlig hälsning

FINANSINSPEKTIONEN

Marie Jesperson
Regelgivningsansvarig

Bilagor:

- Förslag till nya föreskrifter och allmänna råd om hantering av operativa risker,
- Förslag till nya föreskrifter och allmänna råd om it-system, informationssäkerhet och insättningssystem,
- Förslag till ändrade föreskrifter (FFFS 2007:16) om värdepappersrörelse, samt
- Remisspromemoria

Sändlista:
Sveriges riksbank
Kommerskollegium
Riksgäldskontoret
Skatteverket
Pensionsmyndigheten
Kammarkollegiet
Statens tjänstepensionsverk
Statistiska centralbyrån
Konkurrensverket
Konsumentverket
Regelrådet
Riksrevisionen
Advokatsamfundet
Aktiemarknadsbolagens förening
Aktiemarknadsnämnden
Aktiespararna
Bankernas arbetsgivareorganisation
Bankgirocentralen BGC AB
Bokföringsnämnden
Civilekonomerna
Datainspektionen
Euroclear Sweden
FAR
Finansbolagens förening
Finansförbundet
Fondbolagens förening
Föreningen för god sed på värdepappersmarknaden
Företagarnas riksorganisation
Industrins Finansförening
Jusek
Kollegiet för svensk bolagsstyrning
Konsumenternas Bank- och finansbyrå
Landsorganisationen (LO)
Myndigheten för samhällsskydd och beredskap
Nasdaq OMX
Näringslivets regelnämnd
Post- och telestyrelsen
Revisorsnämnden

Rådet för finansiell rapportering
SACO
Sparbankernas Riksförbund
Svensk Försäkring
Svenska Bankföreningen
Svenska Fondhandlareföreningen
Svenska Handelskammarförbundet
Svenskt Näringsliv
Sveriges Redovisningskonsulters förbund

För kännedom
Finansdepartementet
Justitiedepartementet

2013-11-25

R E M I S S P R O M E M O R I A

FI Dnr 11-11528 och 12-4167

Finansinspektionen
Box 7821
SE-103 97 Stockholm
[Brunnsgatan 3]
Tel +46 8 787 80 00
Fax +46 8 24 13 35
finansinspektionen@fi.se
www.fi.se

Förslag till nya regler om hantering av operativa risker samt it-system, informationssäkerhet och insättningssystem

Sammanfattning

Finansinspektionen föreslår två nya föreskrifter som innebär skärpta krav på banker, kreditmarknadsföretag och värdepappersbolag att hantera operativa risker i sin verksamhet på ett effektivt och sunt sätt. Syftet är att minska risken för händelser i företagens verksamhet som resulterar i höga förluster eller omfattande störningar, vilket i sin tur bidrar till att upprätthålla ett stabilt och väl fungerande finansiellt system.

De krav på hantering av operativa risker som finns idag är få och generellt utformade. Finansinspektionen bedömer att det behövs mer precisa regler som ger företagen bättre förutsättningar att på ett strukturerat och systematiskt sätt identifiera, mäta och bedöma operativa risker.

De båda föreskrifterna och allmänna råden om dels hantering av operativ risker, dels it-system, informationssäkerhet och insättningssystem, innebär också att företag ska tillsätta resurser och genomföra åtgärder för att hantera riskerna.

Utöver detta föreslås följdändringar i Finansinspektionens föreskrifter (FFFS 2007:16) om värdepappersrörelse.

Genom förslagen inför Finansinspektionen Baselkommitténs riktlinjer Principles for the sound management of operational risk och delar av Europeiska bankmyndighetens riktlinjer för intern styrning (GL 44) för intern styrning som bindande regler. Dessutom införs särskilda krav på företag som erbjuder tjänster som omfattas av den statliga insättningsgarantin. Dessa syftar till att slutligt anpassa den svenska regleringen till det så kallade insättningsgarantidirektivet.

De nya och ändrade reglerna föreslås träda i kraft den 1 maj 2014.

Innehåll

1 Utgångspunkter

1.1 Bakgrund

I näringsverksamhet kan förluster uppstå när interna processer inte är ändamålsenliga, när personal inte följer processerna eller när it-system upphör att fungera. Det är exempel på händelser som har sitt ursprung i företagens verksamhet. Förluster kan också uppstå på grund av att yttre omständigheter drabbar företaget, till exempel avbrott i elförsörjning, naturkatastrofer och dataintrång. Det gemensamma för dessa är att de har sin orsak i händelser som sker utanför företagets verksamhet.

Operativa risker kan uppstå i alla typer av verksamheter, men arten och omfattningen av dessa risker beror på företagets verksamhetsmodell. Ett företags verksamhetsmodell kan beskrivas som den organisation, de processer, de it-system, den personal och den information som behövs för att företaget ska kunna tillhandahålla de produkter och tjänster som ingår i företagets affärsidé. Ett företag som tillhandahåller sina tjänster på internet exponeras till exempel i stor utsträckning för risken för störningar i it-system. För ett företag som tillhandahåller kontanthantering kan däremot värdetransportrån vara en stor risk.

Sverige har i dag en stor finansiell sektor. Om man jämför de finansiella företagens balansomslutning i relation till BNP är Sveriges finansiella sektor bland de största i Europa (inkluderat storbankernas tillgångar utomlands).[1] De finansiella företagens verksamhetsmodeller utvecklas snabbt, vilket medför ständigt tillkommande källor till operativa risker. Exempel på sådan utveckling är den snabbt växande trenden med utläggning av verksamhet till andra företag, ofta i flera led och över landsgränser.

Den tekniska utvecklingen har gjort det möjligt för företagen att öka automatiseringen och effektiviseringen av sin informationshantering, vilket har inneburit att företagens it-system blivit allt mer komplexa och sammanlänkade, både inom ett företag och mellan företag. En störning i ett verksamhetskritiskt it-system kan därmed få omedelbara och betydande konsekvenser, inte bara för det direkt drabbade företagets verksamhet utan även för andra företag.

Under senare år har det också förekommit riktade angrepp mot finansiella företag genom till exempel dataintrång och överbelastningsattacker. Finansiella företag hanterar stora ekonomiska värden och känslig information och är med detta naturliga mål för den här typen av angrepp.

Operativa risker kan orsaka förluster och störningar som allvarligt kan skada finansiella företag liksom förtroendet för och stabiliteten i hela den finansiella sektorn. Den finansiella sektorn upplevde fram till för knappt 20 år sedan

[1] Riksbankens rapport Finansiell stabilitet (FSR 2013:1), diagram 1.

endast enstaka väsentliga förluster på grund av operativa risker. År 1995 kollapsade Barings Bank på grund av ett omfattande bedrägeri som väckte frågor kring de finansiella företagens sårbarhet och mot risker som skapas i företagens egen verksamhet.

De avregleringar av finansmarknaderna som genomförts från 1980-talet fram till i början på 2000-talet, kombinerat med den snabba produkt- och teknikutvecklingen och gränsöverskridande processer har tydliggjort att det krävs en ny syn på betydelsen av operativa risker som kan uppstå i och orsaka skada inom den finansiella sektorn.

Under 2011 utförde Internationella valutafonden (IMF) en utvärdering av Sveriges finansiella sektor. I slutrapporten konstaterade IMF att Sverige saknar riktlinjer för hantering av operativa risker och rekommenderade att Sverige utvecklar en sådan reglering.[2]

Sammanfattningsvis är därför en ändamålsenlig reglering av de risker som uppstår i de finansiella företagens operativa verksamheter av central betydelse för företagen, konsumentskyddet och den finansiella stabiliteten.

När det särskilt gäller skyddet för inlåningskunder hos företag som tillhandahåller tjänster som omfattas av den statliga insättningsgarantin, finns det sedan mars 2009 ett krav på Riksgäldskontoret (Riksgälden) att kunna betala ut medel ur insättningsgarantin inom tjugo arbetsdagar mot tidigare tre månader om ett finansiellt företag skulle försättas i konkurs. Detta ställer i sin tur krav på att företagen har it-system för att utan dröjsmål kunna sammanställa en fullständig och tillförlitlig förteckning över företagets samtliga insättare och deras respektive insättningar.[3] Riksgälden har gett ut föreskrifter samt en detaljerad handledning om hur förteckningen ska se ut och hur den ska överföras till myndigheten, men det saknas i övrigt regler som ställer krav på de it-system som de finansiella företagen behöver för att sammanställa förteckningen.

1.2 Målet med regleringen

I denna promemoria föreslås två nya föreskrifter som behandlar hur kreditinstitut, det vill säga banker och kreditmarknadsföretag, och värdepappersbolag ska arbeta med operativa risker. För det första – föreskrifter och allmänna råd om hantering av operativa risker som behandlar allmänna krav på hantering av operativa risker samt särskilda krav inom värdepappersrörelse och valutahandel. För det andra – föreskrifter och allmänna råd om it-system, informationssäkerhet och insättningssystem – som

[2] "Emphasis placed on operational risk is not strong as for some other risk areas. This is exemplified by the lack of guidance to firms with respect to operational risk."
IMF Country Report No 11/172 – Sweden: Financial Sector Stability Assessment, s. 47.

[3] Regeringens proposition 2010/11:109. Ändringar av insättningsgarantin. Avsnitt 5.1.

specifikt behandlar hur företag ska arbeta med it-system, informationssäkerhet och insättningssystem.

De nya föreskrifterna syftar till att säkerställa att företagen hanterar sina operativa risker på ett effektivt och sunt sätt. Genom att strukturerat och systematiskt identifiera, mäta och bedöma operativa risker samt tillsätta resurser och genomföra åtgärder för att hantera riskerna, minskar sannolikheten att riskerna omsätts till händelser som orsakar höga och oväntade förluster eller bortfall av intäkter. Det kan handla om att minska sannolikheten för omfattande bedrägerier, förlust av viktig information eller långa kostsamma rättsprocesser.

Genom de båda föreskrifterna införs i Sverige internationella riktlinjer från Baselkommittén för banktillsyn (BCBS) i form av Principles for the sound management of operational risk. Dessutom införs delar av Europeiska bankmyndighetens (Eba) riktlinjer för intern styrning (GL 44).

Genom föreskrifterna om hantering av operativa risker införs Joint Forums[4] High-level principles for business continuity. Även Europeiska banktillsynskommitténs (CEBS)[5] Guidelines on the management of operational risks in market-related activities införs. Med föreskrifterna om hantering av operativa risker bedömer Finansinspektionen att IMF:s rekommendation att Sverige bör ta fram riktlinjer för operativa risker kan anses vara uppfylld vad gäller kreditinstitut och värdepappersbolag.

Genom föreskrifterna om it-system, informationssäkerhet och insättningssystem inför Finansinspektionen regler som syftar till att begränsa de operativa riskerna när det gäller företagens it-system och informationshantering, samt regler som klargör vad ett företag som tar emot medel som omfattas av insättningsgarantin ska uppfylla. Förutom de sistnämnda reglerna om insättningssystem, finns liknande regler om it-system och informationssäkerhet, som de som nu föreslås, sedan lång tid tillbaka i övriga nordiska länder. De regler som föreslås om insättningssystem syftar ytterst till att fullständigt genomföra ändringarna i insättningsgarantidirektivet.[6]

1.3 Nuvarande och kommande regelverk

1.3.1 Nuvarande regler

Ett kreditinstituts verksamhet regleras i huvudsak i lagen (2004:297) om bank- och finansieringsrörelse (LBF). Värdepappersbolagens verksamhet regleras i

[4] http://www.bis.org/bcbs/jointforum.htm

[5] Europeiska banktillsynskommitten är sedan 2011 ersatt av Europeiska bankmyndigheten (Eba).

[6] Jfr Europaparlamentets och rådets direktiv 2009/14/EG av den 11 mars 2009 om ändring av direktiv 94/19/EG om system för garanti av insättningar, vad gäller täckningsnivån och utbetalningsfristen (EUT L 68, 13.3.2009, s. 3, Celex 32009L0014).

huvudsak i lagen (2007:528) om värdepappersmarknaden (LV). De kreditinstitut som har tillstånd att driva värdepappersrörelse ska även följa vissa av bestämmelserna i LV.

Finansinspektionens allmänna råd (FFFS 2005:1) om styrning och kontroll av finansiella företag knyter an till reglerna i LBF genom att övergripande rekommendera hur kontroll av risker bör hanteras. I råden undantas flera olika företagstyper, bland annat värdepappersbolag, från tillämpningsområdet. Finansinspektionen arbetar nu för att även undanta kreditinstitut från de allmänna rådens tillämpningsområde. Avsikten är att kreditinstitut i stället ska tillämpa de kommande föreskrifterna och allmänna råden om styrning, riskhantering och kontroll i kreditinstitut som Finansinspektionen remitterat tidigare under året,[7] och de båda föreskrifter som nu remitteras. Finansinspektionens allmänna råd om styrning och kontroll av finansiella företag ska fortsättningsvis tillämpas av ett begränsat antal företagstyper, till exempel försäkringsföretag.

Organisatoriska krav för värdepappersrörelse finns i Finansinspektionens föreskrifter (FFFS 2007:16) om värdepappersrörelse. Enligt föreskrifterna ska ett värdepappersinstitut bland annat ha riktlinjer och rutiner för riskhantering samt riktlinjer för en avbrottsfri verksamhet, så kallad kontinuitetshantering. Det finns även regler om dokumentation av uppgifter. Här anges bland annat att värdepappersinstitut ska bevara uppgifter om transaktioner så att Finansinspektionen kan rekonstruera viktiga steg i hanteringen av samtliga transaktioner.

Företag som använder mer avancerade metoder för beräkning av kapitalkrav på operativa risker, det vill säga schablon- och internmätningsmetoderna, ska tillämpa vissa begränsade och generella hanteringskrav. Regler om detta finns i Finansinspektionens föreskrifter och allmänna råd (FFFS 2007:1) om kapitaltäckning och stora exponeringar.[8] För närvarande är det tjugo företag som beräknar kapitalkrav enligt schablonmetoden och ett företag som har tillstånd att använda internmätningsmetoden.

I lagen (2006:1371) om kapitaltäckning och stora exponeringar finns bestämmelser som anger att en finansiell företagsgrupp bland annat ska uppfylla kraven om riskhantering i LBF och LV.

1.3.2 Kommande regler

Som nämnts ovan pågår för närvarande ett arbete hos Finansinspektionen med att ge ut nya föreskrifter och allmänna råd om styrning, riskhantering och kontroll i kreditinstitut. Föreskriftsförslagen i denna promemoria har tagits fram parallellt med dessa föreskrifter och allmänna råd.

---

[7] Dnr 11-5610, remissdatum 2013-06-25.

[8] Se 30 kap. 2 § och kap. 44. FFFS 2007:16.

I detta regelarbete har Finansinspektionen även beaktat den pågående internationella regelutvecklingen på området, främst arbetet inom EU med det nya kapitaltäckningsdirektivet (CRD 4)[9] och kapitaltäckningsförordningen (CRR)[10]. Det är till exempel från artikel 85 i CRD 4 som kravet på att ett företag ska tillämpa interna regler och processer för att utvärdera och hantera exponeringen för operativa risker kan härledas. Av samma artikel följer också att ett företag ska ha beredskaps- och affärskontinuitetsplaner för att säkerställa förmågan att löpande driva sin verksamhet och begränsa förlusterna vid en allvarlig störning i verksamheten.

1.4 Ärendets beredning

I arbetet med att ta fram de nya föreskrifterna har Finansinspektionen konsulterat två externa referensgrupper som har bestått av representanter från Svenska Bankföreningen, Sparbankernas Riksförbund, Finansbolagens förening och Svenska fondhandlareföreningen. Finansinspektionen har haft flera möten med dessa. Vidare har Finansinspektionen avseende vissa delar i förslagen rådgjort med Myndigheten för samhällsskydd och beredskap (MSB) och med Riksbanken.

Därutöver har Finansinspektionen när det gäller föreskrifterna om hanteringen av operativa risker, inom ramen för referensgruppens arbete, vid ett tillfälle träffat enskilda företag verksamma inom värdepappersområdet för att särskilt diskutera förslagets sjätte kapitel om operativa risker inom viss värdepappersrörelse och valutahandel.

När det gäller föreskriftsförslaget om it-system, informationssäkerhet och insättningssystem har Finansinspektionen även rådgjort med Riksgälden och Datainspektionen.

1.5 Regleringsalternativ

Finansinspektionen har övervägt om det finns andra möjligheter att säkerställa att företagen hanterar sina operativa risker samt att de upprätthåller tillräcklig säkerhet för att kunna fullgöra kraven på insättningssystem, än genom att införa bindande regler på området.

Det finns redan i dag riktlinjer från Eba och rekommendationer från CEBS, BCBS och Joint Forum.

---

[9] Europaparlamentets och rådets direktiv 2013/36/EU av den 26 juni 2013 om behörighet att utöva verksamhet i kreditinstitut och om tillsyn av kreditinstitut och värdepappersföretag, om ändring av direktiv 2002/87/EG och om upphävande av direktiv 2006/48/EG och 2006/49/EG.

[10] Europaparlamentet och rådets förordning (EU) nr 575/2013 av den 26 juni 2013 om tillsynskrav för kreditinstitut och värdepappersföretag och om ändring av förordning (EU) nr 648/2012.

Eba:s riktlinjer GL 44 omfattar som tidigare nämnts även hanteringen av operativa risker. Dessa riktlinjer är att betrakta som allmänna råd som företag kan avvika från om de kan visa att syftet med råden uppfylls även med det sätt som företaget väljer att arbeta med riskerna. BCBS har lämnat viss vägledning om hanteringen av operativa risker. Dessa vägledningar har inte den normerande verkan som Eba:s riktlinjer har, utan ska ses som rekommendationer. Det finns också etablerade standarder på it- och informationssäkerhetsområdena som berör hantering av specifika operativa risker. Till exempel finns COBIT-ramverket för it-styrning, ITIL (IT Infrastructure Library) som är ett ramverk för hantering av it-tjänster och svensk standard "Ledningssystem för informationssäkerhet – Krav" enligt SS-ISO/IEC 27001. Variationerna i de nämnda regelverkens normerande funktioner är enligt Finansinspektionens uppfattning problematisk, dels ur ett tillämpningsperspektiv, dels ur ett tillsynsperspektiv.

Ett alternativ till att ge ut nya föreskrifter är att överlåta till branschen att själva reglera området, möjligen med vägledningar från Finansinspektionen som komplement. Det finns dock så pass stora skillnader mellan företagen att Finansinspektionen bedömer det svårt att uppnå en sådan samsyn att självreglering blir effektivt. Utan bindande regler på en ändamålsenlig detaljnivå ges alltför stort utrymme för tolkningar, vilket försvårar för företagen att tillämpa reglerna och för Finansinspektionen att bedriva tillsyn och föra dialog med företagen. Ytterst är det samhället och konsumenterna som får bära kostnaderna när riskhanteringen inte fungerar tillfredställande.

Eftersom hanteringen av operativa risker kostar pengar finns det en uppenbar risk att företag inte ger området tillräckligt med uppmärksamhet. Operativa risker som omvandlas i inträffade incidenter kan medföra betydande kostnader för företag, konsumenter och samhället. Finansinspektionen återkommer till detta i den konsekvensutredning som finns i avsnitt 6 i denna promemoria. Redan nu kan dock sägas att den betydelse som operativa risker har hos finansiella företag talar för att en tydlig reglering på området är nödvändig. Finansinspektionens uppfattning är därför att en bindande reglering om hantering av operativa risker är nödvändig för att skapa en godtagbar nivå på hanteringen av riskerna inom hela kollektivet av kreditinstitut och värdepappersbolag.

När det gäller insättningssystem så saknas det detaljerade krav som ålägger företagen att ha it-system som är tillräckligt säkra för hantering av uppgifter om insättare. Utan regler på en tillräcklig detaljnivå finns det små möjligheter för Finansinspektionen att åstadkomma förbättringar i företagens hantering av denna information. Det skulle i princip vara upp till företagen själva att avgöra om de i händelse av fallissemang kan infria det behov som Riksgälden har på informationens tillförlitlighet och fullständighet. Finansinspektionen anser det därför nödvändigt att införa bindande regler om insättningssystem. Det är dessutom nödvändigt för att fullständigt genomföra ändringarna i insättningsgarantidirektivet.

1.6 Rättsliga förutsättningar

Enligt 6 kap. 2 § första stycket LBF ska ett kreditinstitut identifiera, mäta, styra, internt rapportera och ha kontroll över de risker som dess rörelse är förknippad med. Företaget ska se till att det har en tillfredsställande intern kontroll. Motsvarande bestämmelser finns för värdepappersbolag i 8 kap. 4 § första stycket LV.

Vidare finns det för kreditinstituten i 6 kap. 3 a § LBF krav på att kreditinstitut ska ha system för hantering av uppgifter om insättare och deras insättningar som ska vara sådana att kreditinstitutet utan dröjsmål kan sammanställa en fullständig och tillförlitlig förteckning över företagets samtliga insättare och deras respektive insättningar. Motsvarande bestämmelser finns för värdepappersbolag i 8 kap. 36 § LV.

I 16 kap. 1 § 3 LBF samt 5 kap. 2 § 4 förordningen (2004:329) om bank- och finansieringsrörelse finns bemyndiganden för Finansinspektionen att meddela föreskrifter om vilka åtgärder som ett kreditinstitut ska vidta för att uppfylla de krav på soliditet och likviditet, riskhantering, genomlysning, sundhet samt riktlinjer och instruktioner som avses i 6 kap. 1–5 §§ LBF.

I 8 kap. 42 § 2 LV samt 6 kap. 1 § 9 värdepappersmarknadsförordningen (2007:572) finns bemyndiganden för Finansinspektionen att meddela föreskrifter om vilka åtgärder som ett värdepappersinstitut ska vidta för att uppfylla de krav på soliditet och likviditet, riskhantering och genomlysning samt riktlinjer och instruktioner som avses i 8 kap. 3–8 §§ LV.

I 8 kap. 42 § 3–6 LV samt 6 kap. 1 § 10–13 värdepappersmarknadsförordningen (2007:572) finns bemyndiganden för Finansinspektionen att meddela föreskrifter om vilka åtgärder som ett värdepappersinstitut ska vidta för att uppfylla de krav på de riktlinjer, regler och rutiner ett värdepappersinstitut ska upprätta och tillämpa enligt 8 kap. 9 § LV, vilka system, resurser och rutiner ett värdepappersinstitut ska ha enligt 8 kap. 10 § LV, vad ett värdepappersinstitut ska iaktta för att uppfylla skyldigheterna i 8 kap. 11 § LV och dokumentation enligt 8 kap. 12 § LV.

När det gäller krav på insättningssystem hos värdepappersbolag finns bemyndiganden i 6 kap. 1 § 29 förordningen om värdepappersmarknaden för Finansinspektionen att meddela föreskrifter, det vill säga krav som är kopplade till 8 kap. 36 § LV.

Som tillägg till ovanstående finns för värdepappersbolag även bestämmelser i 8 kap. 10 § LV som anger att värdepappersinstitut ska ha tillräckliga system, resurser och rutiner för att kunna tillhandahålla investeringstjänster och utföra investeringsverksamhet kontinuerligt och regelbundet. Till bestämmelsen finns i 6 kap. 1 § 11 förordningen om värdepappersmarknaden ett bemyndigande kopplat som ger Finansinspektionen rätt att föreskriva om vilka system, resurser och rutiner ett värdepappersinstitut ska ha för att uppfylla dessa krav.

Enligt 8 kap. 11 § 4 LV ska ett värdepappersinstitut ha en effektiv drift och förvaltning av sina informationssystem. Även till denna bestämmelse finns ett bemyndigande kopplat i 6 kap. 1 § 12 förordningen om värdepappersmarknaden som ger Finansinspektionen rätt att föreskriva om vad ett värdepappersinstitut ska iaktta för att uppfylla skyldigheterna i 8 kap. 11 § LV.

De föreskrifter om operativa risker och om insättningssystem som här föreslås, är en integrerad beståndsdel av riskhantering samt system för hantering av uppgifter om insättare och deras insättningar. De föreslagna föreskrifterna bedöms därför rymmas inom de bemyndiganden som Finansinspektionen har enligt ovan.

1.7 Ikraftträdande

Föreskrifterna föreslås träda i kraft den 1 maj 2014.

Finansinspektionen föreslår inte några övergångsregler.

2 Motivering och överväganden

2.1 Tillämpningsområde och definitioner

2.1.1 Vilka företag omfattas och varför

De nya föreskrifterna och allmänna råden föreslås bli tillämpliga för kreditinstitut, det vill säga banker och kreditmarknadsföretag, och värdepappersbolag. I dag träffar regelförslagen totalt 259 företag under Finansinspektionens tillsyn. Av dessa är 89 banker, 45 kreditmarknadsföretag och 125 värdepappersbolag.

I förslaget till föreskrifter om hantering av operativa risker ska kapitel 6 om särskilda krav på hantering av operativa risker inom värdepappersrörelse och valutahandel, gälla för de företag som har tillstånd till investeringstjänster och investeringsverksamheter i enlighet med 2 kap. 1 § p.1–4 LV. Det innebär att detta kapitel förutom värdepappersbolag med dessa tillståndstyper även gäller kreditinstitut med de tillstånden. De kreditinstitut som bedriver valutahandel med stöd av 7 kap. 1 § 12 LBF, ska också tillämpa reglerna i kapitlet.

Kapitel 3, insättningssystem, i förslaget till föreskrifter om it-system, informationssäkerhet och insättningssystem gäller endast för de företag som tar emot eller avser att ta emot medel som omfattas av insättningsgarantin.

Förslaget till föreskrifter om hantering av operativa risker kommer i viss omfattning att införa bestämmelser motsvarande de som redan finns för värdepappersbolag i Finansinspektionens föreskrifter (FFFS 2007:16) om värdepappersrörelse. För att inte värdepappersbolagen ska omfattas av två olika regelverk med samma innehåll, har Finansinspektionen undantagit värdepappersbolagen från vissa av de bestämmelser som föreslås. Vilka dessa bestämmelser är framgår av 1 kap. 3 § i föreskrifterna om hantering av operativa risker.

2.1.2 Definitioner

I föreskrifterna finns det behov av definitioner.

Det för föreskrifterna centrala begreppet *operativ risk* avses omfatta detsamma som operativ risk enligt artikel 4.1 i CRR, nämligen *risken för förluster till följd av ej ändamålsenliga eller fallerade processer, människor, system eller yttre händelser, inbegripet legala risker.* I stället för att skriva ut definitionen görs en hänvisning till CRR.

I de fall samma begrepp används i båda dessa föreskrifter som i förslaget till föreskrifter och allmänna råd för styrning, riskhantering och kontroll i kreditinstitut föreslås de ha samma innebörd oavsett vilken föreskrift de finns i.

Det åstadkoms genom hänvisningar från de båda föreskrifterna till föreskrifterna och allmänna råden för styrning, riskhantering och kontroll i kreditinstitut.

Föreskrifterna om it-system, informationssäkerhet och insättningssystem hänvisar dessutom till föreskrifterna om hanteringen av operativa risker när det gäller begreppen incident och process.

I övrigt finns självständiga definitioner i respektive föreskrift.

2.1.3 Tillämpning av reglerna på finansiell företagsgrupp.

Tills vidare föreslår Finansinspektionen att föreskrifterna inte ska tillämpas på finansiella företagsgrupper.

Den 1 januari 2014 träder CRR i kraft. Samtidigt pågår ett regelarbete för att genomföra CRD 4 i Sverige. Det senare kommer dock inte att vara klart till den 1 januari 2014. Dessa två regelverk förväntas i viss mån ändra innebörden av finansiell företagsgrupp och hur den ska hanteras i riskhänseende. Eftersom den slutliga svenska texten för genomförandet i lag inte är klar, avstår Finansinspektionen i detta läge från att i föreskriftsförlagen föreslå gruppbestämmelser.

2.2 Proportionalitet

Av förarbetena till 6 kap. LBF och 8 kap. LV framgår att de krav som ställs på företagen enligt bestämmelserna om soliditet och likviditet, riskhantering och genomlysning kan variera med de verksamheter som företagen ägnar sig åt. Bestämmelserna i 6 kap 1–3 §§ LBF och 8 kap. 3–5 §§ LV ska enligt 6 kap. 4 a § samma lag och enligt 8 kap. 6 § LV omfattas av proportionalitet och enligt förarbetena till dessa bestämmelser bör Finansinspektionen beakta proportionalitetsprincipen vid utformning av inspektionens föreskrifter.[11]

En effektiv riskhantering grundar sig på att företagen anpassar sina metoder eller rutiner efter verksamhetens art, omfattning och komplexitet. I arbetet med att utforma förslaget till nya föreskrifter har Finansinspektionen beaktat denna lagreglerade proportionalitetsprincip. Det framgår därför av några av de föreslagna reglerna att företagen ska ta hänsyn till vissa faktorer när de utformar sina processer, metoder eller interna regler. I praktiken innebär det att alla företag ska uppfylla bestämmelserna i föreskrifterna men att det kan göras på olika sätt. För företag med mer komplex verksamhet är det naturligt att det till exempel finns fler kontroller än för ett företag med en mindre komplex verksamhet. För en effektiv och sund riskhantering ska företagen alltid utgå

[11] Prop. 2002/03:39 s. 275, 277 och 279 f och prop. 2006/07:215 (i fråga om värdepappersbolagen).

från sin egen verksamhet i riskhanteringen och dimensionera hanteringen därefter.

3 Förslag till nya föreskrifter och allmänna råd om hantering av operativa risker

I detta avsnitt redogör Finansinspektionen för väsentliga delar av förslaget till föreskrifter och de överväganden som har gjorts. I vissa fall kommenteras enskilda paragrafer och begrepp. Redogörelsen följer samma ordning som kapitlen i de föreslagna föreskrifterna, nämligen följande:

- styrning och ansvar (2 kap.),
- identifiering och mätning (3 kap.),
- rapportering (4 kap.),
- hantering av operativa risker i verksamheten (5 kap.), och
- särskilda krav på hantering av operativa risker inom värdepappersrörelse och valutahandel (6 kap.).

3.1 Styrning och ansvar (2 kap.)

Kapitlet innehåller grundläggande bestämmelser om hur ett företag ska hantera den övergripande styrningen av operativa risker.

Finansinspektionens utgångspunkt är att ett företags hantering av sina operativa risker är av sådan betydelse för företagets överlevnad att det bör åligga styrelsen att säkerställa att riskerna hanteras på ett ändamålsenligt sätt och att riskhanteringen får den fokus som krävs i organisationen. Finansinspektionen föreslår därför regler om att det är styrelsens ansvar att besluta om risktoleransen för operativa risker och om interna regler för att hantera dessa.

Det krav som Finansinspektionen föreslår på att ett företag ska ha interna regler för hantering av operativa risker är baserat på artikel 85 i CRD 4 som anger att ett företag ska tillämpa riktlinjer och processer för att utvärdera och hantera exponeringen för operativa risker.

Verksamheter kan ha olika komplexitet och omfattning. Finansinspektionen föreslår att ett företag ska ta hänsyn till detta när det utformar de interna reglerna. Det framgår av den proportionalitetsregel som finns i 2 kap. 2 § fjärde stycket. På så sätt kan företaget anpassa metoderna för att identifiera och mäta de operativa riskerna för olika verksamheter. För vissa slag av risker kan det till exempel vara lämpligt med en årlig risk- och sårbarhetsanalys för att identifiera och mäta risken, medan en lämplig metod för andra risker kan vara en analys av förluststatistik.

3.2 Identifiering och mätning (3 kap.)

Det grundläggande kravet på att identifiera och mäta operativa risker finns i 6 kap. 2 § LBF. Identifieringen och mätningen är en förutsättning för att företaget ska kunna hantera riskerna på ett planlagt sätt. En viktig aspekt i sammanhanget är också att identifiering och mätning av riskerna ger företaget möjlighet att dels se samband mellan olika typer av brister och operativa risker, dels att följa upp om de åtgärder som vidtas ger avsedd effekt. En fragmenterad och ofullständig bild av de operativa riskerna försvårar en ändamålsenlig riskhantering. Ett företag behöver därför på en tillräckligt detaljerad nivå ha kunskap om sina väsentliga operativa risker.

De föreslagna kraven på mätning av operativa risker innebär inte att ett företag nödvändigtvis ska utveckla egna kvantitativa beräkningsmodeller. Syftet är däremot att se till att företaget har kriterier och mått (både kvantitativa och kvalitativa) som det tillämpar systematiskt vilket ger företaget en möjlighet att följa hur riskerna utvecklas. Finansinspektionen föreslår därför att ett företag ska fastställa indikatorer för operativa risker och gränsvärden för dessa vilket syftar till att ge en förvarning om när den operativa risken har ökat.

I allmänna råd till paragrafen om indikatorer och gränsvärden ges exempel på ett antal indikatorer som kan användas i flera olika former av verksamheter. Ett företag behöver givetvis utveckla och anpassa indikatorerna till dess specifika verksamhet och de risker som följer av denna.

Hantering och uppföljning av incidenter är en viktig pusselbit vid identifiering och mätning av operativa risker. Därför bör ett krav finnas på att företaget ska analysera och dokumentera uppgifter om de incidenter och de förluster som har uppstått. Genom detta skapas möjlighet att få fram information om de bakomliggande orsakerna, till exempel om orsakerna är isolerade eller återkommande händelser, samt hur de bäst bör hanteras.

Som tidigare nämnts i denna promemoria finns idag en snabbt växande trend med utläggning av verksamhet till andra företag, så kallad outsourcing. Finansinspektionens utgångspunkt är att det alltjämt är det uppdragsgivande företaget som ansvarar för riskerna och riskhanteringen i verksamheten även om den är i vissa delar drivs av ett annat företag. Ett uppdragsgivande företag behöver därför samla in information om incidenter och förluster även i den utlagda verksamheten. Denna information är viktig för att företaget i tid ska kunna vidta lämpliga åtgärder i fråga om riskhanteringen. I föreskriftsförslaget finns därför ett krav på sådan insamling av information.

3.3 Rapportering (4 kap.)

I tillsynsverksamheten har Finansinspektionen iakttagit brister i företagens rapportering av operativa risker till styrelser och verkställande direktörer, både

när det gäller rapporternas innehåll och omfattning. Finansinspektionen har också iakttagit att det finns stora skillnader i företagens interna rapportering av operativa risker. Hos en del företag rapporteras endast förluststatistik, medan andra företag tar fram omfattande och detaljerade rapporter. Innehållsrika rapporter är bra men det finns också en risk att alltför omfattande och detaljerade rapporter kan vara svåra att tillgodogöra sig och använda som underlag till beslut om åtgärder. Finansinspektionen föreslår därför vissa grundläggande krav på den information som ska ingå i rapporteringen till styrelsen och den verkställande direktören när det gäller operativa risker. Detta rapporteringskrav gäller utöver de krav som redan finns på rapportering av risker i 6 kap. 7 § i värdepappersföreskrifterna och 5 kap. 5 § och 6 kap. 7–8 §§ Finansinspektionens förslag till föreskrifter och allmänna råd om styrning, riskhantering och kontroll i kreditinstitut.

3.4 Hantering av operativa risker i verksamheten (5 kap.)

Det femte kapitlet i föreskrifterna innehåller regler för hur ett företag ska hantera operativa risker i verksamheten.

3.4.1 Processer

De produkter och tjänster som ett företag tillhandahåller tas fram genom en kedja av aktiviteter, definierad som processer. Många gånger, speciellt i stora företag, utförs olika aktiviteter i processer av olika personer, inte sällan inom olika organisatoriska enheter. Finansinspektionen har lagt märke till att delar av processer hos ett flertal företag på senare år har flyttats till andra länder eller lagts ut på underleverantörer.

Enligt den statistik som Finansinspektionen har tillgång till för år 2011 och 2012 för de fyra storbankerna i Sverige uppgår de operativa förlusterna relaterade till processer till ungefär 50 procent av det totala förlustbeloppet orsakat av operativa risker. Även internationell förluststatistik visar på samma förhållande.[12]

Brister i företagets processer uppstår av olika anledningar. Det kan handla om ineffektiva kontroller i processen, att processen inte följs eller att den inte är anpassad till gällande regler.

Eftersom inte alla processer på ett företag är av väsentlig betydelse föreslår Finansinspektionen att företaget fastställer vilka de processerna är och att dessa processer dokumenteras. Exempel på sådana processer kan vara processen för kreditgivning, processen för betalningar eller processen för rådgivning. Givetvis kan även företagets stödprocesser vara av väsentlig betydelse, till exempel processer för riskkontroll eller myndighetsrapportering.

[12] Till exempel The Operational Riskdata eXchange Association (ORX) rapport 2012 "ORX Report on operational risk loss".

Genom att processerna dokumenteras bör riskerna i dem bli tydliggjorda och en effektiv hantering av dessa risker möjliggörs. Det skapar förutsättningar för ett riskbaserat arbetssätt och för en ändamålsenlig prioritering av resurser.

Finansinspektionen lämnar även allmänna råd om vad grundläggande dokumentation av processer bör innehålla.

Finansinspektionen föreslår att regeln ska tillämpas proportionellt. Det innebär till exempel att det för ett mindre företag kan betyda att företaget dokumenterar ett begränsat antal processer där den sammanlagda processdokumentationen är på ett fåtal sidor, medan det för en storbank kan handla om ett stort antal processer där gemensamma standarder för dokumentation av processerna kan behöva utvecklas.

3.4.2 Personal

Personalbrist, brist på kompetens eller oklar arbetsfördelning är vanliga orsaker till fel och misstag som ett företags personal gör. När det gäller operativa risker förknippade med personal är det särskilt viktigt att riskhanteringen inriktas på förebyggande aktiviteter. Finansinspektionen föreslår därför att ett företag ska ha ett antal rutiner för att hantera operativa risker förknippade med personalen.

Finansinspektionen anser att ett företag till exempel ska kontrollera uppgifter i samband med nyanställning av personal. Det kan handla om inhämtande av referenser eller verifiering av uppgifter om till exempel andra uppdrag som en person har vid sidan av den sökta tjänsten. Vilken typ av kontroll som bör utföras beror på företagets verksamhet och vilken tjänst eller funktion som anställningen gäller. Risken för intressekonflikter är något som särskilt ska beaktas.

En annan situation är att det finns personal med kompetens som är svår att ersätta med kort varsel och som är nödvändiga för företagets verksamhet. Det kan till exempel handla om personer med särskilda kunskaper om specifika it-system eller personer som dagligen utför viktiga kontroller. För ett företag kan det vara viktigt att den funktion som en viss person fyller är säkerställd även om den personen är frånvarande.

I sin tillsynsverksamhet har Finansinspektionen sett att det är viktigt att befattningsbeskrivningar, limiter och mandat är tydligt fastställda och uppdaterade. När detta inte är gjort ökar risken för onödiga fel eller att viktiga arbetsuppgifter inte tas om hand. Det är särskilt tydligt vid omorganisationer och vid hög personalomsättning. Ett företag föreslås därför vara skyldigt att ha rutiner om befattningsbeskrivningar, limiter och mandat.

Finansinspektionen föreslår också att det ska finnas rutiner för att identifiera och hantera operativa risker som kan uppstå när personal internt byter arbetsuppgifter eller enheter. Exempel på en förflyttning som kan behöva

hanteras är när en anställd som i sin tidigare roll haft mandat att genomföra transaktioner som medför marknads- eller kreditrisker för företaget, börjar arbeta på funktionen för riskkontroll. Om personen i fråga kontrollerar sina tidigare transaktioner skulle det kunna innebära en risk för manipulering av data.

3.4.3 Legala risker

Ett område som kan orsaka höga direkta förluster eller omfattande ryktesproblem är bristande hantering av legala risker. Finansinspektionen föreslår därför att ett företag ska ha interna regler för sin hantering av legala risker. Reglerna ska säkerställa att det finns ett strukturerat arbetssätt med dessa frågor på företaget.

3.4.4 It-system

Förslag till regler om hantering av dessa finns i förslaget till föreskrifter om it-system, informationssäkerhet och insättningssystem, se avsnitt 4 i denna promemoria.

3.4.5 Säkerhetsarbete

Den finansiella sektorn hanterar tillgångar av stort värde och är därför särskilt utsatt för brottsliga handlingar, till exempel rån eller bedrägerier. Det är därför viktigt att ett företag identifierar de tillgångar som behöver skyddas från så väl externa som interna hot.

Det är inte rimligt att tro att alla typer av brott kan förebyggas, men med en ändamålsenlig riskhantering och effektiva kontroller kan riskerna reduceras. Finansinspektionen föreslår därför genom allmänna råd metoder som ett företag bör använda i sitt förebyggande säkerhetsarbete.

Information, särskilt om kunder och transaktioner, är en av de viktigaste tillgångarna i ett finansiellt företag och den behöver därför skyddas. Detaljerade regler kring informationssäkerhet finns i förslaget till föreskrifter om it-system, informationssäkerhet och insättningssystem, se avsnitt 4 i denna promemoria.

3.4.6 Process för godkännande

Införande av nya produkter, tjänster, processer, it-system eller genomförande av omorganisationer är en naturlig och viktig del av affärs- och verksamhetsutvecklingen. Ett företags exponering för operativa risker ökar i regel när det exempelvis införs nya produkter eller görs större förändringar. Även om syftet med att till exempel ändra eller införa en ny process eller ett nytt it-system på längre sikt kan vara att minska risken i verksamheten, är själva förändringen alltid förknippat med en ökad risk. Genom att ett företag har fastställda processer för godkännande av förändringar ges möjlighet att

brister och risker upptäcks i tid, vilket bör ge företaget möjlighet att agera förebyggande.

Bestämmelserna om processen för godkännande är till stora delar baserade på avsnitt 23 i GL 44, samt på riktlinjerna om godkännande i BCBS Principles for the sound management of operational risk. Medan GL 44 fokuserar på riktlinjer för godkännande av nya marknader, produkter och tjänster, omfattar BCBS riktlinjer även processer och system.

Finansinspektionen har övervägt att i föreskriftsförslaget separera processerna för godkännande på de områden som omfattas av GL 44 från de områden som tillkommer från BCBS riktlinjer. Emellertid är frågor kring godkännande ofta integrerade med varandra. Införande av en ny produkt kan till exempel innebära att ett företag också behöver införa eller förändra processer och it-system. Finansinspektionen har därför stannat vid att i förslaget ha reglerna om processer som baseras på GL 44 respektive BCBS riktlinjer tillsammans.

I sin tillsyn har Finansinspektionen sett att ett företag kan ha behov av att utvärdera förändringar för att kunna dra lärdom om positiva och negativa effekter av förändringen. Finansinspektionen föreslår därför en regel om att ett beslut om godkännande av till exempel en ny produkt ska dokumenteras. Genom dokumentation skapas möjlighet att i efterhand utvärdera processerna.

3.4.7 Kontinuitetshantering

Det kan finnas många orsaker till ett avbrott eller en större störning i ett företags verksamhet vilket kan leda till att företaget inte kan fullgöra sina skyldigheter gentemot sina kunder och andra marknadsaktörer. Oavsett vad som är orsak till avbrottet eller störningen behöver ett företag ha förmåga att hantera ett avbrott eller en större verksamhetsstörning så att det kan återgå till normal verksamhet inom rimlig tid. En väl fungerade kontinuitetshantering är viktigt, inte bara för företaget utan även dess kunder och det finansiella systemet som helhet. Finansinspektionen föreslår därför att företaget ska ha interna regler för kontinuitetshantering. För att kontinuitetshantering ska ges det fokus och de resurser som krävs för att vara väl fungerande föreslår Finansinspektionen att reglerna ska beslutas av företagets verkställande direktör. Ett företag ska också ha en skyldighet att ta fram beredskaps-, kontinuitets- och återställningsplaner. De regler som Finansinspektionen föreslår om kontinuitetshantering är främst baserade på riktlinjerna i avsnitt 31 i GL 44.

För att ta fram ändamålsenliga beredskaps-, kontinuitets- och återställningsplaner samt företagets prioriteringar och mål under återställningsskedet ska ett företag enligt förslaget, analysera de konsekvenser som ett avbrott eller en större verksamhetsstörning kan ha på verksamheten. Planerna är viktiga att fastställa i förväg då resurserna för att återställa en verksamhet efter ett avbrott eller en störning ofta är begränsade.

Det är viktigt att företaget kan kommunicera effektivt med relevanta interna och externa parter vid större verksamhetsstörningar. Detta gäller i synnerhet i inledningen av en störning för att företaget ska kunna bedöma störningens effekter. När en störning uppstår behöver företaget även fatta lämpliga beslut om huruvida beredskapsplaner, kontinuitetsplaner och återställningsplaner ska användas eller inte. Med tanke på detta och med hänsyn till den ökade press som ställs på beslutsfattare i samband med större verksamhetsstörningar, föreslår Finansinspektionen att krav på rutiner för intern och extern kommunikation införs som en del av kontinuitetshanteringen.

Förutom att beredskaps-, kontinuitets- och återställningsplaner ska uppdateras föreslår Finansinspektionen att det införs ett krav på tester. Testerna är viktiga för att bedöma om planerna är tillräckliga och för att öka personalens kunskap om hur dessa ska användas.

Värdepappersbolagen har undantagits från att tillämpa de föreslagna reglerna om kontinuitetshantering eftersom detta område regleras i värdepappersföreskrifterna, se avsnitt 2.1.1.

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

Finansinspektionen föreslår att reglerna i kapitel 6 i föreskrifterna ska tillämpas på de företag som har tillstånd att tillhandahålla investeringstjänster och utföra investeringsverksamheter enligt med 2 kap. 1 § 1–4 LV och på företag som driver valutahandel med stöd av 7 kap. 1 § 12 LBF i den verksamhet som är förknippad med dessa tillstånd.

De regler som föreslås i kapitlet är i första hand baserade på CEBS Guidelines on the management of operational risks in market related activities. Det finns i dag ingen officiell definition av vad som avses med marknadsrelaterade aktiviteter. Finansinspektionen har därför valt att avgränsa området till de verksamheter som faller inom ramen för de investeringstjänster och investeringsverksamheter som framgår av 2 kap. 1 § 1–4 LV och verksamheter med valutahandel som utförs med stöd av 7 kap. 1 § 12 LBF.

Syftet med att ställa mer specifika krav på hantering av operativa risker i dessa verksamheter, är att de är särskilt utsatta för operativa risker. Verksamheterna är ofta komplexa samtidigt som de omsätter höga belopp och stora volymer. Konsekvenser av bristande hantering eller bedrägerier kan snabbt leda till stora skador för ett företag och dess kunder. Sedan den omfattande tradingsincidenten i Barings Bank 1995 har det förekommit flera incidenter som har resulterat i stora ekonomiska förluster för de drabbade företagen. Incidenterna kan skada inte bara det enskilda företaget och dess kunder utan hela marknaden, eftersom förtroendet för värdepappersmarknaden kan urholkas.

3.5.1 Åtskillnad av arbetsuppgifter

För att förebygga att operativa risker uppstår i verksamheter med värdepappersrörelse och valutahandel föreslår Finansinspektionen regler som syftar till att säkerställa åtskillnad av arbetsuppgifter i fråga om transaktionshantering, det vill säga att den som utför en transaktion inte ska kontrollera sitt eget arbete.

3.5.2 Personal

För att öka möjligheten att upptäcka eventuella oegentligheter eller felaktigheter föreslås att personal som initierar och genomför affärstransaktioner inte ska hantera transaktioner under minst 10 arbetsdagar i en följd under loppet av ett år. Denna bestämmelse ska även gälla personal i funktionen för riskkontroll och stödfunktioner kopplade till den positionstagande enheten.

Bestämmelsen införs mot bakgrund av att många förluster i dessa verksamheter har uppstått till följd av att personer med god insikt i hur företagets system fungerar (till exempel handlare med ett förflutet inom stöd- eller kontrollfunktion) under en längre tid har kunnat dölja växande förluster i felaffärer eller rena bedrägerier. Om personal i vissa positioner inte har möjlighet att hantera sina vanliga transaktioner under en sammanlagd tidsperiod på åtminstone 10 arbetsdagar per år blir det lättare för ett företag att upptäcka denna typ av manipulationer.

3.5.3 Transaktionshantering

För att ett företag ska kunna upptäcka, utreda och analysera olika typer av fel eller avvikelser föreslås regler kring verifieringskedjan för varje transaktion. Till exempel föreslås en regel om skriftlighet och verifiering av motparten vid hantering av transaktioner där motparten önskar villkor som avviker från företagets normala rutiner. Genom detta bör risken minska för till exempel att affärer måste makuleras därför att avveckling inte kan ske mot den aktuella motparten.

För att undvika osäkerhet, minimera ekonomiska konsekvenser vid felaffärer och minska risken för missförstånd, ska ett företag sträva efter att så långt som möjligt inte ha affärer som är obekräftade. Därför föreslås krav som innebär att bekräftelser ska utbytas med motpartens stödfunktion eller funktion för riskkontroll så snart som möjligt. Detta är viktigt också för att säkerställa att det inte råder oenighet om vilken part som står för risken.

Om obekräftade affärer ändå uppstår, ska ett företag ha fastställda rutiner för hantering och rapportering av dessa. Rutinerna bör bland annat ange de åtgärder som ska vidtas för att kunna få affären bekräftad, vem som vidtar

åtgärderna, vem som bedömer risken i den obekräftade affären samt vem som fattar beslut om vad som ska göras om affären till exempel måste ligga obekräftad över natten och vilka personer i företaget som ska informeras.

Finansinspektionen föreslår också ett krav på daglig avstämning av transaktioner, likvider och positioner. Även konton och portföljer som inte är aktiva ska stämmas av eftersom det alltid finns en risk att positioner medvetet eller omedvetet registreras på dessa så länge de inte är spärrade för registrering.

3.5.4 Hantering av säkerheter

Finansinspektionen föreslår regler avseende hantering av säkerheter. Företaget ska kontrollera säkerheter, till exempel att de är korrekta genom att de överensstämmer med de positioner som kunder har eller som företaget har i eget lager.

Med ett krav på att ett företag har system för sammanställning av utnyttjade limiter kan risken för överträdelser av motpartlimiter minskas.

3.5.5 Övervakning

Finansinspektionens utgångspunkt är att ett företag ska utföra övervakning av värdepappers- och valutahandeln på ett sådant sätt och med en sådan frekvens att företaget har en så heltäckande bild av sina risker som möjligt. Företaget bör därigenom kunna upptäcka felaktigheter, felbedömningar och bedrägliga aktiviteter på ett så tidigt stadium som möjligt.

Föreskriftsförslaget anger att väsentliga avvikelser och resultat vid värdepappershandel ska analyseras för att bedöma huruvida de beror på händelser som är hänförliga till operativa risker eller inte. Granskningen bör utgå från bedömningen av huruvida resultatet är rimligt utifrån de mandat och limiter som gäller för den granskade verksamheten samt med hänsyn tagen till vid varje tidpunkt rådande marknadsförutsättningar.

I föreskrifterna föreslås att interna konton löpande ska granskas och stämmas av. Liksom vid den dagliga avstämningen är det viktigt att såväl aktiva som passiva konton och depåer kontrolleras. Syftet med bestämmelsen är att dels att säkerställa att företaget inte har okända risker till exempel genom positioner på vilande men fortfarande öppna konton, dels att säkerställa att företaget fångar upp bedrägliga aktiviteter i form av transaktioner eller positioner som medvetet göms eller flyttas runt mellan depåer eller interna konton.

När portföljer och "tradingböcker" granskas förekommer det att man förenklar och enbart granskar nettopositionen och inte de i nettot ingående positionerna. Eftersom denna metod inte nödvändigtvis identifierar alla operativa risker förknippade med positionerna föreslår Finansinspektionen att kontroller av värdet på nettopositioner kompletteras med kontroll av de transaktioner som ger upphov till dessa. Tanken är att kunna göra en djupare analys av riskbilden

i positionen och att fånga upp misstag, felbedömningar eller medveten manipulering av positionen.

Finansinspektionen föreslår att företaget ska fastställa och regelbundet följa upp sina limiter för positioner på en sådan detaljerad nivå att uppföljning och kontroll kan göras till exempel per handlare, tradingbok eller portfölj. På det sättet kan företaget dels kontrollera att uppsatta limiter följs, dels spåra vem som brutit mot limiten eller vad som är orsaken till överträdelsen.

Finansinspektionen föreslår i en bestämmelse att företaget minst kvartalsvis ska kontrollera behörigheter till it-system inom värdepappersrörelsen och valutahandel. Förslaget till kvartalsvisa kontroller har sin bakgrund i att denna verksamhet är extra utsatt för operativa risker och kontroller av behörigheter är en viktig åtgärd för att hantera risken. Bestämmelsen är således strängare än den bestämmelse i 3 kap 7§ i förslaget till föreskrifter om it-system, informationssäkerhet och insättningssystem, se avsnitt 4 i denna promemoria.

4 Förslag till nya regler om it-system, informationssäkerhet och insättningssystem

Finansinspektionen redogör nedan för de väsentliga delarna av föreskriftsförslaget och de överväganden som gjorts.

De regler som föreslås i kapitel 2 och 3 kompletterar föreskrifterna om hantering operativa risker avseende krav för hantering av it-system och informationssäkerhet. Det tredje kapitlet om insättningssystem behandlar krav på företag som tar emot insättningar som omfattas av lagen (1995:1571) om insättningsgaranti.

Motiveringarna är i huvudsak övergripande och tas upp samma ordning som kapitlen i de föreslagna föreskrifterna. I vissa fall kommenteras enskilda paragrafer och begrepp.

Redogörelsen följer samma ordning som kapitlen i de föreslagna föreskrifterna, nämligen följande:

- it-system,
- informationssäkerhet, och
- insättningssystem.

4.1 It-system (2 kap.)

De regler som föreslås i kapitlet tar sikte på hanteringen av företagens it-system. Det handlar om att de tekniska systemen ska ha en viss säkerhet, att det ska finnas en tydlig målsättning för företagets it-verksamhet, att ansvaret för verksamheten är tydligt och att det ska finnas ändamålsenliga processer och rutiner för hanteringen av systemen.

4.1.1 Säkra it-system

Det har tidigare i denna promemoria framhållits att finansiella företag allt mer är beroende av it-system för att hantera sin information och för att upprätthålla sin verksamhet. Det finns därför enligt Finansinspektionen ett behov av en portalparagraf som klargör att företagen ska ha it-system som är säkra.

Denna portalparagraf knyter an till den grundläggande regeln om att ett företag ska ha ändamålsenliga it-system och rutiner för att skydda konfidentialitet, riktighet och tillgänglighet i dess information. För kreditinstitut finns denna regel i 2 kap. 2 § i de föreslagna föreskrifterna och allmänna råden om styrning, riskhantering och kontroll i kreditinstitut och för värdepappersbolag i 6 kap. 2 § Finansinspektionens föreskrifter (FFFS 2007:16) om värdepappersrörelse.

Ett företag ska ha ändamålsenliga it-system och rutiner för att skydda konfidentialitet, riktighet och tillgänglighet i dess information. Dessa system och rutiner ska ta hänsyn till den berörda informationens art.

Ett finansiellt företag har vanligtvis många olika it-system för sin verksamhet och vissa system är mer verksamhetskritiska än andra. Vilken säkerhetsnivå ett it-system ska ha kan till exempel kopplas till hur viktigt systemet är för verksamheten eller vilken sekretess som gäller informationen i systemen. Vad som är tillräckligt säkert måste därför bedömas från fall till fall. En utgångspunkt är att koppla denna bedömning till den information som it-systemet hanterar. I förslagets tredje kapitel föreslår Finansinspektionen att ett företag ska klassificera sin information utifrån krav på konfidentialitet, riktighet och tillgänglighet. När det gäller bedömningen om it-systemen är tillräckligt säkra föreslår Finansinspektionen därför ett allmänt råd med innebörden att företagen bör utgå från klassificeringen av informationen när det bedömer kraven på it-systemen.

4.1.2 Mål och strategi

De övergripande målen och strategierna för ett företags verksamhet fastställs normalt av företagets styrelse. Det är naturligt att företagets arbete inom it-verksamheten, inköp och utveckling av it-system, underhåll och drift följer och stödjer företagets övriga verksamhet. För att säkerställa att it-verksamheten utvecklas i samma riktning som företagets övriga verksamheter måste det enligt Finansinspektionen finnas tydliga mål även för denna verksamhet.

It-verksamhet är per definition inte en direkt intäktskälla för finansiella företag utan en kostnad som utgör stödfunktion för de intjänande verksamheterna i företagen. Genom att föreskriva att mål och övergripande strategier för it-verksamheten ska fastställas av ett företags verkställande direktör förutsätts att it-frågor ges den uppmärksamhet som behövs för att verksamheten ska fungera,

samt att mål och långsiktigt arbete med it-verksamheten går i samma riktning som den övriga verksamheten.

4.1.3 Processer

Utan klara och tydliga processer och rutiner för it-verksamheten saknas förutsättningar för ett strukturerat och kontrollerat arbetssätt. Genom att dokumentera processerna minskar även personberoenden i verksamheten och en intern kunskapsbank säkerställs. Finansinspektionen föreslår därför krav på att det ska finnas dokumenterade processer.

Vilka processer som ska vara dokumenterade kan variera mellan olika företag. De företag som inte själva utvecklar sina it-system behöver inte ha processer för systemutveckling, medan det för andra företag är viktigt för kvaliteten i it-systemen att det finns dokumenterade processer för detta arbete. Ett företag som köper in it-system behöver säkerställa att de krav som företaget har på it-systemen uppfylls. Genom ett allmänt råd anger Finansinspektionen ett antal processer som bör finnas dokumenterade.

Behovet av dokumentationen kan variera från process till process. Finansinspektionen föreslår därför en proportionalitetsbestämmelse kopplad till att det ska finnas dokumenterade processer. Proportionaliteten avser utformningen och dokumentationen av processerna och inte att vissa av kraven på processer kan väljas bort. Ett företag har således flexibilitet att tillämpa kraven utifrån allmänt etablerade principer, standarder och ramverk på området samt företagets egna förutsättningar.

En närmare redogörelse för de processer som bör dokumenteras enligt förslaget följer nedan.

Inköp, utveckling och förvaltning
Bristande kvalitet i it-system, såväl vid egenutveckling som vid inköp av standardsystem, kan få stora konsekvenser. Vid sidan av risken för att systemet kan fallera kan bristande kvalitet få konsekvenser som inte alltid härleds till it-systemen. Exempelvis kan dåligt utformade gränssnitt för inmatning av data göra att risken för mänskliga misstag ökar och dåligt utformade applikationskontroller kan öka risken för bedrägerier. Införande av ett bristfälligt system i syfte att stödja en verksamhetsprocess kan i värsta fall medföra ökade operativa risker. Det är därför viktigt att ett företag inte bara i samband med inköp och utveckling, utan också vid underhåll av it-system har ändamålsenliga processer.

Drift
Driften av ett it-system är förknippad med många dagliga och regelbundna aktiviteter. Brister i dessa kan få stora konsekvenser på riktigheten och tillgängligheten hos det data som systemen hanterar. Finansinspektionen föreslår därför att ett företag bör ha dokumenterade processer och rutiner för driften. Med process för drift avses att de åtgärder och funktioner som behövs

för den dagliga driften av företagets it-system bör vara formaliserade och att arbetet med driften i så stor utsträckning som möjligt ska kunna följas upp i efterhand.

Incidenthantering
Incidenter av varierande grad som påverkar ett företags it-system inträffar regelbundet. För att företagets it-system ska kunna återställas till en normal drift vid händelse av en incident relaterad till ett it-system, föreslås att ett företag ska ha en process för incidenthantering. Processen syftar bland annat till att mildra effekterna av incidenter genom att ett företag har en effektiv och sammanhållen hantering av incidenter som påverkar dess it-system, samt att de brister i it-verksamheten som har lett till incidenten åtgärdas för att förhindra att de upprepas.

Ändringshantering
Bristande rutiner vid ändringshantering är en vanlig orsak till driftsavbrott. För att minska risken för driftsavbrott, obehöriga ändringar och fel är det viktigt att företaget hanterar ändringar på ett kontrollerat sätt. Finansinspektionen föreslår därför att ett företag bör ha en process för att hantera ändringar som kan påverka företagets it-system.

Test av it-system
Ett företag behöver säkerställa att ett it-system uppfyller de krav som företaget har på systemet. Företaget bör för detta ändamål ha en fastställd process för test av it-system. Det kan till exempel handla om utformning av testaktiviteter, testplaner och rapportering av testresultaten. Finansinspektionen föreslår därför att det bör finnas i en dokumenterad process för test av it-system.

Uppdragsavtal (outsourcing)
I it-samanhang är det vanligt med uppdragsavtal, det vill säga att företag lägger ut hela eller delar av sin it-verksamhet på annan. Finansinspektionen vill med denna upplysningsbestämmelse tydliggöra att det finns regler om uppdragsavtal i annan reglering som är tillämpliga vid utläggning av it-verksamhet.

4.2 Informationssäkerhet (3 kap.)

Informationssäkerhet syftar till att skydda information. Med att skydda information avses i detta förslag att kunna upprätthålla rätt nivå av konfidentialitet, riktighet och tillgänglighet.

Att åstadkomma och upprätthålla tillräcklig säkerhet är en komplex process som omfattar hela företagets verksamhet, både när informationen hanteras manuellt och när informationen hanteras med hjälp av it-system. En tillräcklig informationssäkerhet är samtidigt en förutsättning för att kunna utnyttja de möjligheter den tekniska utvecklingen ger på ett effektivt och förtroendeskapande sätt.

4.2.1 *Ledningssystem för informationssäkerhet*

Finansinspektionen anser att ett strukturerat och metodiskt arbete med informationssäkerhet är en förutsättning för att skapa och upprätthålla informationssäkerhet. Då information, särskilt om kunder och transaktioner, är en av ett företags viktigaste tillgångar anser Finansinspektionen att det är ett rimligt krav att ett företag arbetar strukturerat och metodiskt med att skydda informationens säkerhet.

Som nämnts tidigare finns det etablerade standarder för att underlätta ett systematiskt arbete med informationssäkerhet. Detta kan man till exempel göra genom att införa ett ledningssystem för informationssäkerhet enligt svensk standard SS-ISO/IEC 27001. Finansinspektionen har valt att beakta svensk standard "Ledningssystem för informationssäkerhet – Krav" enligt SS-ISO/IEC 27001:2006 i samband med utformande av de föreslagna reglerna. Detta innebär emellertid inte att Finansinspektionen ställer krav på att ett företag ska införa och certifiera sig mot denna standard. Finansinspektionen är emellertid positiv till användningen av standarder som stöd i ett företags arbete med informationssäkerhet.

4.2.2 *Mål och inriktning*

För att informationssäkerhetsarbetet ska ges det fokus och de resurser som krävs, föreslår Finansinspektionen att ett företags mål och inriktning med informationssäkerhetsarbetet ska beslutas av företagets verkställande direktör eller styrelse.

4.2.3 *Informationsklassificering och riskanalys*

Informationssäkerhet definieras i de föreslagna reglerna som skydd av konfidentialitet, riktighet och tillgänglighet hos information. All information hos ett företag är inte lika värdefull och kritisk när det gäller dessa tre kriterier. Därför kan det finnas anledningar, inte minst av kostnadsskäl, för ett företag att tillämpa olika skyddsnivåer beroende på hur värdefull och kritisk informationen är. Klassificering av företagets information är därför viktig för att informationen och it-systemen ska få lämplig skyddsnivå.

Genom att klassificera sin information och analysera sina risker kan ett företag fatta relevanta beslut om lämpliga skyddsåtgärder för informationen i verksamheten.

4.2.4 *Interna regler*

I denna regel föreslås en proportionalitetsregel där företagen ska beakta arten, omfattningen och komplexiteten i sin verksamhet när det utformar de interna reglerna för informationssäkerhet. Genom proportionalitetsregeln tydliggörs att olika företags interna regler för informationssäkerhet kan ha, och i realiteten ofta har, olika omfattning och utformning.

I samband med kravet att det ska finnas fastställda interna regler föreslår Finansinspektionen allmänna råd om vad de interna reglerna om informationssäkerhet bör omfatta. Råden bör underlätta företagens arbete att ta fram egna interna regler.

Vilka krav de interna reglerna enligt förslaget bör ange redogörs för nedan.

Fysisk säkerhet
Utan tillräckliga skyddsåtgärder för fysisk säkerhet kan små incidenter få omfattande konsekvenser. Detta gäller särskilt för lokaler som inrymmer verksamhetskritisk utrustning som till exempel serverhallar. Tillträdesskydd och skydd mot annan yttre påverkan som till exempel brand, översvämning och störningar i elförsörjningen är exempel på skyddsåtgärder. Bristande tillträdesskydd till känsliga lokaler kan medföra att obehöriga individer ges fysisk tillgång till stora mängder känslig data eller utrustning som gör det möjligt att kringgå existerande skyddsåtgärder.

Skydd av datakommunikation och drift
För att säkerställa en säker drift av ett företags it-system är det viktigt att förhållanden som är av betydelse för driften av företagets it-system och datakommunikationen som förbinder dessa beaktas ur ett säkerhetsperspektiv.

Finansinspektionen anser i sammanhanget att det är viktigt att företaget fastställer krav på vilka aktiviteter i it-systemen som ska vara spårbara. Det syftar till att det i efterhand ska vara möjligt att spåra aktiviteter som är av betydelse för säkerheten i företagets it-system. Exempel på sådana aktiviteter som bör vara spårbara kan vara skapande och borttagande av användarkonton i systemet, förändring av kontons behörighet eller åtkomst till känsliga objekt. För att förhindra obehörig åtkomst till eller ändringar i företagets driftsmiljö, samt driftsavbrott bör ett företag även fastställa den nivå på separation mellan driftmiljö respektive test- och utvecklingsmiljöer som är nödvändig för att säkerställa en säker drift av företagets it-system.

Säkerhetskrav på it-system vid inköp, utveckling och underhåll
För att säkerställa att informationssäkerheten integreras i företagets it-system är det viktigt att ett företag tar hänsyn till verksamhetens säkerhetskrav i samband med inköp, utveckling och underhåll av it-system.

Incidentrapportering och incidenthantering
För att kunna vidta rätt åtgärder i tid i samband med incidenter som är relaterade till företagets informationssäkerhet är det viktigt att företaget har rutiner för rapportering och för hur incidenter ska hanteras. Sådana rutiner syftar bland annat till att mildra effekterna av incidenter och underlätta återgång till normal drift samt att de brister i verksamheten som har lett till incidenten åtgärdas för att förhindra att de upprepas.

Genom rapporteringen av informationssäkerhetsrelaterade incidenter säkerställs att incidenterna inkluderas i företagets arbete med att dokumentera och analysera incidenter och förluster samt orsakerna till dessa, så som föreslås i 3 kap. 6 § Finansinspektionens förslag till föreskrifter om hantering av operativa risker.

Regelbunden kontroll av den fastställda skyddsnivån
Den föreslagna regeln om regelbunden kontroll syftar till att säkerställa att den fastställda skyddsnivån återspeglas i praktiken. Finansinspektionen anser att principerna för företagets kontroll bör fastställas i företagets interna regler.

4.3 Insättningssystem (4 kap.)

4.3.1 Tillämpningsområde

Föreskrifternas fjärde kapitel, om insättningssystem, syftar till att närmare utveckla de krav på system för hantering av insättare och deras insättningar som framgår av 6 kap. 3 a § LBF och 8 kap. 36 § LV. De företag som omfattas av kraven har således att både ta hänsyn till de allmänna krav som ställs i andra och tredje kapitlet i föreskrifterna och de särskilda krav som ställs i det fjärde kapitlet.

Det skäl som ligger bakom förslaget på särskilda krav för insättningssystem är Riksgäldens ökade behov att i princip redan vid tidpunkten för insättningsgarantins inträde kunna förlita sig på fullständigheten och tillförlitligheten hos den information som företagen hanterar i sina insättningssystem. Genom de ändringar i EU-kommissionens insättningsgarantidirektiv som antogs 2009 måste Riksgälden sedan 2011 kunna betala ut ersättning från insättningsgarantin inom 20 arbetsdagar från tidigare tre månader.[13]

Reglerna i detta kapitel följer den struktur som presenteras i regeringens proposition 2010/11:109 om ändringar i insättningsgarantin gällande utformningen av krav på it-system för hantering av information om insättare och deras insättningar.[14]

4.3.2 Riskanalyser

Ett företag ska identifiera skyddsåtgärder för att uppnå en tillräcklig säkerhet avseende dels den information om insättare och deras insättningar som hanteras i it-systemet, dels för systemets integritet.

---

[13] Se Europaparlamentets och rådets direktiv 2009/14/EG av den 11 mars 2009 om ändring av direktiv 94/19/EG om system för garanti av insättningar.

[14] Se prop. 2010/11:109 s. 37.

De skyddsåtgärder som företaget identifierar genom riskanalys tillsammans med de funktioner och rutiner som anges i 4 kap. 4 § första stycket ska vara tillräckliga för att säkerställa fullständigheten och tillförlitligheten i den information om insättare och deras insättningar som systemet hanterar.

4.3.3 Funktioner och rutiner

För att ett it-system ska kunna betraktas som tillförlitligt är det viktigt med spårbarhet, det vill säga att det är möjligt att utläsa vilka aktiviteter som har gjorts i it-systemet och vilka ändringar som har gjorts av systemet samt när och av vem. Det är då nödvändigt att ett företag har ändamålsenliga tekniska funktioner och administrativa rutiner för detta ändamål.

Med kravet om att aktiviteter i systemet ska vara spårbara avses såväl transaktionsuppgifter, uppgifter om insättare, som ändringar av systemparametrar som kan påverka insättningssystemets funktion och säkerhet.

För att skydda de tekniska funktionerna för åtkomstkontroll och spårbarhet är det viktigt att ett företag även har ändamålsenliga tekniska funktioner för att säkerställa systemets integritet.

4.3.4 Granskning

Skyddet av informationen och informationens fullständighet och tillförlitlighet är central för kunder och konsumenter. Det är dessa som direkt påverkas om ett företag, i en omtumlande situation som en konkurssituation eller när företaget annars inte kan återbetala förfallna fordringar, inte förmår att leverera information om insättarna och deras fordringar på företaget till Riksgälden. Enligt Finansinspektionens uppfattning är det därför lämpligt att hanteringen av insättningssystem årligen granskas av ett företags funktion för internrevision.

5 Följdändringar i andra föreskrifter och allmänna råd

5.1 Finansinspektionens föreskrifter (FFFS 2007:16) om värdepappersrörelse

De nu föreslagna föreskrifterna ska förutom för kreditinstitut gälla även för värdepappersbolag. Finansinspektionen föreslår därför vissa mindre ändringar i föreskrifterna om värdepapperrörelse i de delar som specifikt rör frågor som är relaterade till eller täcks av de nu föreslagna föreskrifterna om it-system, informationssäkerhet och insättningssystem.

Till följd av användningen av de på informationssäkerhetsområdet vedertagna begreppen konfidentialitet, riktighet och tillgänglighet i den föreslagna föreskriften om it-system, informationssystem och insättningssystem, föreslås en anpassning av terminologin i 6 kap. 2 § föreskrifterna om värdepappersrörelse. Detta innebär ingen förändring i sak.

5.2 Finansinspektionens allmänna (FFFS 2011:50) råd om ansökan om tillstånd att driva bank- eller finansieringsrörelse

Finansinspektionens allmänna råd om ansökan om tillstånd att driva bank- eller finansieringsrörelse innehåller bland annat allmänna råd om hur en ansökan om tillstånd att driva bank- eller finansieringsrörelse bör vara utformad, samt vilken information en sådan ansökan bör innehålla. Eftersom de nu föreslagna reglerna kommer att utgöra bindande regler är information kring hur ett ansökande företag avser att följa reglerna något som Finansinspektionen kommer att behöva kontrollera. De allmänna råden om ansökan om tillstånd att driva bank- eller finansieringsrörelse behöver därför ändras för att omfatta det nya behov av information som de nya föreskrifterna ger upphov till.

Då Finansinspektionen avser att göra en större översyn av de allmänna råden om ansökan om tillstånd att driva bank- eller finansieringsrörelse, som dock inte ryms inom ramen för detta regelgivningsprojekt, föreslås för närvarande inga förändringar i de allmänna råden.

6 Förslagets konsekvenser

6.1 Berörda företag

De företag som ska följa de föreslagna reglerna är kreditinstitut och värdepappersbolag. I dag finns det totalt 259 sådana företag under Finansinspektionens tillsyn. Av dessa är 89 banker, 45 kreditmarknadsföretag och 125 värdepappersbolag.

6.2 Konsekvenser för företagen och marknaden

Finansinspektionen har i detta avsnitt gjort vissa uppskattningar av tillkommande kostnader för att införa de föreslagna nya föreskrifterna och välkomnar ytterligare uppgifter från företagen under remissförfarandet. Detta gäller särskilt i fråga om uppgifter om kostnader för mindre företag.

Riskhantering är förknippad med kostnader för företagen. Å andra sidan kan bristande riskhantering kosta betydligt mer, såväl för företaget självt som för andra aktörer. Det visar inte minst tradingincidenten i banken Société Générale 2008 där företaget rapporterade förluster på ca 46 miljarder kronor.[15] I fallet Barings Bank 1995 uppgick förlusterna till över 15 miljarder kronor.[16]

Kostnaderna kopplade till de föreslagna bestämmelserna består både av fasta och löpande kostnader. För ett enskilt företag kan kostnaderna vara beroende av i vilken grad företagets nuvarande processer och metoder är utformade i enlighet med svenska och internationella riktlinjer och standarder. Om befintliga processer och metoder baseras på sådana regelverk bör kostnaden för anpassning till de föreslagna föreskrifterna bli lägre än annars.

För företagen innebär båda de nya föreskrifterna att företagen behöver göra en översyn av sin befintliga riskhantering för att kartlägga om, och i så fall vilka förändringar som är nödvändiga att göra. Eftersom bestämmelserna till stor del bygger på olika internationella rekommendationer som funnits på området i flera år har ett flertal företag, sannolikt framför allt större företag, redan gjort en del av det arbetet. Dock måste även dessa företag gå igenom och noggrant säkerställa att deras verksamhet uppfyller kraven i föreskrifterna. För företag som bedömer att de i huvudsak redan idag uppfyller reglerna kommer således kostnaderna förknippade med förslagen huvudsakligen vara begränsade till att säkerställa detta och av en engångskaraktär. För andra företag kan det krävas mer arbete för att ta fram och fastställa nya interna regler och rutiner. En del

[15] Société Générale, Årsredovisning 2008, s 154.
http://www.societegenerale.com/sites/default/files/documents/soc006drf08va.pdf
[16] Riksbankens rapport Finansiell stabilitet (FSR 2000:2), s. 49.

företag kan också komma att behöva investera i nya tekniska system eller rekrytera ytterligare personal.

Som framgår av tidigare avsnitt i promemorian föreslår Finansinspektionen att en proportionalitetsprincip ska gälla avseende vissa av föreskrifternas bestämmelser. Beroende på företagets art, omfattning och komplexitet samt exponering mot operativa risker och nuvarande ramverk för hantering av operativa risker kan införandet av de nya föreskrifterna därmed föranleda olika stora löpande kostnader. Nedan redogörs för de materiella, administrativa och finansiella kostnader som de nya reglerna kan komma att föranleda.

6.2.1 Materiella kostnader

De regler som föreslås kan innebära att företag väljer att använda stöd i form av it-system. Kostnader för investeringar i sådana system är exempel på materiella kostnader.

Många företag samlar redan idag in information om incidenter och förluster med stöd av olika it-system. Även om reglerna inte explicit ställer krav på att företag ska använda it-system, bortsett från kravet för insättningar som omfattas av insättningsgarantin, är det rimligt att anta att större företag som ännu inte har infört automatiserade lösningar för insamling av uppgifter om incidenter och förluster kommer att välja att göra det.

Kostnader förknippade med investeringar i säkra it-system är generellt svåra att uppskatta eftersom systemen kan vara av olika komplexitet och omfattning. En investering i it-system medför också andra kostnader som till exempel eventuella utvecklingskostnader och konsultkostnader för införande av systemet. Kostnaderna är sannolikt till stora delar av engångskaraktär, även om uppdateringar och löpande underhåll av it-systemen också krävs.

Enkla rapporteringssystem utan krav på hög informationssäkerhet kan ha mycket låg investerings- och införandekostnad, medan investeringar i avancerade analysverktyg med höga krav på flexibilitet kan medföra betydande kostnader för ett företag.

Med antagandet att ett större företag som ännu inte infört en automatiserad lösning för insamling av uppgifter om incidenter och förluster väljer att göra det, bedöms detta kunna medföra en kostnad av engångskaraktär på mellan 50 000 kr och 500 000 kr. I det fall ett företag väljer att utnyttja redan befintliga it-system samt kan anpassa och införa denna lösning med befintlig personal kan engångskostnaden bli mycket begränsad. I det fall ett större företag väljer att köpa in ett mer avancerat och flexibelt systemstöd kan kostnaden för detta komma att bli högre. Som dock påpekats tidigare finns det inga krav på automatiserade lösningar.

6.2.2 *Administrativa kostnader*

Som nämnts tidigare innebär de nya reglerna ett behov av att se över, ändra och i många fall utöka den interna rapporteringen till bland annat styrelse och ledning. Nya rutiner och processer kommer att behöva införas och styrdokument och interna regler tas fram. Detta kommer att föranleda kostnader för företagen, inte minst i inledningsskedet. Kostnaderna som de båda föreskrifterna ger upphov till hos ett företag styrs i hög grad av i vilken mån företagets verksamhet redan är anpassat till befintliga internationella rekommendationer och riktlinjer.

Finansinspektionen gör bedömningen att de flesta företag har interna regler för hantering av risker som till delar motsvarar de krav som Finansinspektionen föreslår i föreskriftsförslagen. Finansinspektionen bedömer också att företagens arbete med de föreslagna interna reglerna även delvis ryms inom ramen för det arbete som företagen redan kan behöva initiera för att uppfylla krav i de föreskrifter som Finansinspektionen föreslår om styrning och kontroll i kreditinstitut.

Med antagande att det tar i snitt en arbetsvecka att uppdatera/utveckla en intern regel så att den är anpassad till föreskriftsförslagens krav, kan kostnaden för detta beräknas uppgå till cirka 50 000 kr för ett företag (*40 timmar x 1 300 kronor*). I föreskriftsförslagen föreslås att ett företag ska ha åtta interna regler. Kostnaden för ett genomsnittligt företag att uppdatera eller utveckla dessa regler kan uppgå till cirka 400 000 kr (*50 000 kr x 8 interna regler*). Då 259 företag berörs av föreskriftsförslaget uppskattas kostnaden för arbetet med interna regler uppgå till 103 600 000 kr (*259 företag x 400 000 kr*).

Vad gäller den interna rapporteringen är bedömningen att det främst är i inledningsskedet som kostnaderna uppkommer. När rapporteringsrutinen sedan är på plats bör den löpande kostnaden vara begränsad. Det är dock rimligt att anta att någon form av incidentrapportering till ledning och styrelse sker redan idag, om än inte nödvändigtvis i en strukturerad form. Det är således viktigt att poängtera att rapporteringskostnader redan idag förekommer, även i företag som inte har formella rutiner för rapportering av incidenter. Det är inte heller orimligt att anta att den löpande kostnaden för rapportering hos ett sådant företag är i samma storleksordning, eller till och med högre, än vad som kommer att bli fallet när de nya reglerna är på plats. Det beror på att avsaknad av tydliga processer och rutiner för hur rapporteringen ska ske sannolikt innebär en större tidsåtgång för att få fram och sammanställa informationen, samt att rapporteringen sker på olika sätt varje gång. Sammantaget bör således kostnaderna med anledning av de nya reglerna om rapportering vara oförändrade, eller till och med lägre än idag hos vissa företag.

I vilken mån företag kommer att behöva anställa ny personal, utbilda befintlig personal eller genomföra organisationsförändringar beror dels på om organisationen redan är anpassad till de rekommendationer och riktlinjer som

reglerna bygger på, dels i vilken grad befintlig personal redan har den kompetens som anses nödvändig. Finansinspektionen bedömer att behovet av nyanställning för att uppfylla krav i föreskriftsförslagen bör vara begränsat. För ett flertal företag bör det snarare handla om omprioriteringar av arbetsuppgifter för befintlig personal.

Finansinspektionens erfarenhet är att företag redan idag vidareutbildar sin personal inom riskhantering, till exempel avseende metoder för riskidentifiering, informationssäkerhet, kontinuitetshantering och godkännande av nya produkter. De nya föreskriftsförslagen bör därför inte föranleda nya betydande kostnader för utbildningar. Finansinspektionen bedömer att kostnaden för utbildning inom aktuella områden ryms inom utbildningsbudgeten för ett genomsnittligt företag.

6.2.3 Finansiella kostnader

De nya föreskrifterna bedöms inte ge upphov till några nya finansiella kostnader i form av till exempel avgifter, ökad upplåningskostnad eller skatter för företagen.

6.2.4 Särskilt om mindre företag och konkurrensen på marknaden

Mindre företag drabbas ofta hårdare av ny reglering eftersom en relativt sett större andel av dessa företags resurser måste användas till regelefterlevnad. Mindre företag saknar också i större utsträckning själva den kompetens som behövs enligt regelverken och kan behöva anlita konsulter.

I de nya föreskrifterna finns i vissa bestämmelser en möjlighet för företagen att beakta sin verksamhets art, omfattning och komplexitet när de anpassar sig till regelverket. Exempel på detta är möjligheten för företag att anpassa sitt informationssäkerhetsarbete till en för verksamheten motiverad nivå. Samtidigt som reglerna innebär krav på företaget ger denna proportionalitetsprincip visst utrymme för att tillämpa en regel utifrån sina egna förutsättningar. Därmed ges möjlighet till skillnader mellan företagen och att risken för att mindre företag drabbas hårdare minskar.

När det gäller de krav som ställs på it-system och informationssäkerhet kan dessa innebära att företag behöver utöka sin administration. Det är dock inte ovanligt ett mindre företag köper sådana funktioner från specialistföretag. De nya föreskrifterna bör då inte innebära några väsentliga extra kostnader för företaget, även om viss omförhandling av avtalen kan behöva göras. Ett mindre företag som har egen administration kan komma att behöva se över denna.

De krav på it-system för att hantera information om insättare och deras insättningar som föreslås i kapitlet om insättningssystem förväntas särskilt för ett mindre företag kunna innebära en ökad kostnad. Det kan antas att mindre företag i högre grad än större företag har insättningssystem som är av sådan art att vidareutveckling eller inköp av ett nytt it-system bedöms som nödvändigt

för nå upp till kraven. Någon proportionalitet föreslås inte beträffande dessa regler eftersom varje företag måste kunna uppfylla dessa krav. Emellertid har ett mindre företag ofta mindre komplexa system och rutiner att ta hänsyn till, vilket bör innebära att företaget har lägre kostnader än ett större företag för att anpassa sina it-system till de föreslagna reglerna. Det är också rimligt att anta att de nya reglerna kan komma att öka tröskeln något för ett mindre företag som planerar att driva inlåningsverksamhet som omfattas av den statliga insättningsgarantin. Finansinspektionen anser emellertid att de föreslagna kraven är väl motiverade mot bakgrund dels av kraven i 6 kap. 3 a § LBF och 8 kap. 36 § LV, dels av Riksgäldens behov av att kunna betala ut ersättning från insättningsgarantin inom 20 arbetsdagar från det att Finansinspektionen konstaterat att en insättare inte har fått insättningar utbetalda från företaget.

Det ska också framhållas att en viss konkurrensobalans kan uppstå i och med att filialer till utländska kreditinstitut inte omfattas av de föreslagna kraven på insättningssystem. Finansinspektionen saknar dock bemyndigande att föreskriva om regler för dessa filialer. I dag finns det 30 filialer till utländska kreditinstitut i Sverige. Fyra av dem har konton som omfattas av den svenska insättningsgarantin.

6.2.5 Sammanfattning om kostnader

Förlusterna som uppkom under 2012 hos de fyra storbankerna i Sverige och som kan knytas till operativa risker uppgick till cirka 350 000 000 kr. Statistiken omfattar dock endast enskilda registrerade förluster som översteg 25 000 kronor. Den sammanlagda volymen av förluster som understiger detta gränsvärde är okänt, men den kan antas vara betydande. Det saknas också samlad förluststatistik avseende förluster som kan knytas till operativa risker hos övriga företag. Det som dock kan konstateras är att de samlade förlusterna är höga.

Kostnaderna för sällan förekommande incidenter av allvarlig art hos finansiella företag är svåra att uppskatta, men som exemplet med Barings Bank visar med förluster på 15 miljarder kronor, kan de bli avsevärda.

De administrativa kostnaderna för branschen att uppdatera interna regler kan uppskattas till 103 600 000 kronor. Detta är dock endast en typ av kostnad som de föreslagna reglerna kan komma att medföra.

Att med säkerhet kvantifiera den totala kostnaden för företagen är omöjligt då de berörda företagens verksamheter har mycket olika omfattning och komplexitet. För vissa företag innebär de föreslagna bestämmelserna sannolikt liten kostnad då företaget redan följer dem, medan det för andra företag kan innebära en väsentlig kostnad om bestämmelserna införs.

Samtidigt bör ett strukturerat och effektivt riskhanteringsarbete över tiden sänka kostnaderna för operativa förluster. Företagen bör få färre kundklagomål och bättre beslutsunderlag i sin verksamhetsstyrning och investeringsplanering.

I många företag uppstår dessutom inte endast kostnader genom förluster på grund av bristande riskhantering, utan även kostnader utifrån hur ett företag väljer att organisera sin riskhantering. Finansinspektionen bedömer att ett företag genom att införa de föreslagna reglerna i vissa fall även kan reducera sina kostnader för hantering av operativa risker genom att arbeta med riskhantering metodiskt.

Som tidigare nämnts kan kostnader för bristande riskhantering bli omfattande både för det enskilda företaget och dess kunder. De föreslagna föreskrifterna förväntas minska riskerna för incidenter som kan härledas till operativa risker och samtidigt öka företagens motståndskraft att hantera avbrott och störningar. Finansinspektionen bedömer därför att de kostnader som kan uppstå i samband med att företagen stärker sin riskhantering genom införande av de föreslagna reglerna är motiverade.

6.3 Konsekvenser för samhället och konsumenten

Konsekvenser av realiserade operativa risker kan direkt påverka konsumenterna och samhället. Till exempel kan en störning i ett verksamhetskritiskt it-system få omedelbara och betydande konsekvenser för ett företags verksamhet på ett sätt som gör att företagets kunder inte kan utnyttja dess tjänster.

Störningar som påverkar stabiliteten på de finansiella marknaderna är ovanliga. Men konsekvenserna kan potentiellt sett bli mycket svåra att hantera om systemviktiga företag drabbas. I förlängningen kan grundläggande samhällsfunktioner påverkas, såsom möjligheterna att betala ut lön och pensioner. Beroende på företagens verksamheter och den realiserade risken kan följdverkningar bli såväl små som omfattande. Ett exempel på det senare, som inte huvudsakligen är från det finansiella området men som ändå kan illustrera effekter av operativa risker, är driftstörningen hos Tieto i november 2011 då omkring 50 företag och myndigheter drabbades.[17]

Eftersom operativa risker potentiellt kan skapa omfattande negativa konsekvenser för samhället bör en effektiv hantering av dessa risker bidra till ett stabilare finansiellt system, ett bra förtroende för företagen och branschen hos kunder och investerare. En effektiv hantering av operativa risker bör även bidra till att företagen får god beredskap att hantera oväntade händelser och att viktiga samhällsfunktioner (betalsystem, kapitalmarknad m.m.) kan upprätthållas.

[17] Reflektioner kring samhällets skydd och beredskap vid allvarliga it-incidenter, En studie av konsekvenserna i samhället efter driftstörningen hos Tieto i november 2011, Myndigheten för samhällsskydd och beredskap, 2012.

Det kan inte uteslutas att ökade kostnader för företagen kommer att föras över till konsumenterna genom exempelvis ökade avgifter. Samtidigt gör Finansinspektionen bedömningen att företagen även kan göra besparingar i form av minskade förluster. Vilken eventuell kostnad som förs över på konsumenterna beror följaktligen på hur företagen kommer att agera och hur stora kostnader reglerna innebär.

6.4 Konsekvenser för Finansinspektionen

Redan i dag utövar Finansinspektionen tillsyn över företagens hantering av operativa risker som en del av den ordinarie tillsynen. Denna tillsyn grundas i viss mån på regler som är generella, vilket gör det mer resurskrävande att utöva en effektiv tillsyn. Eftersom förslagen till föreskrifter innehåller nya och skärpta krav på företagen bedömer Finansinspektionen att de nya reglerna kommer att underlätta och effektivisera tillsynen på detta område.

Tillsynen av företagens hantering av operativa risker och insättningssystem kommer att behöva ses över och utökas. Bland annat kommer det finnas ett behov av att utveckla nya tillsynsrutiner på de områden som inte tidigare varit reglerade på samma detaljnivå. Därutöver kommer sannolikt, i varje fall initialt, antalet förfrågningar från berörda företag att öka med anledning av föreskrifterna.