2014-04-11

B E S L U T S P R O M E M O R I A

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

FI Dnr 11-11528 och 12-4167

Nya regler om hantering av operativa risker samt informationssäkerhet, it-verksamhet och insättningssystem i kreditinstitut och värdepappersbolag

Sammanfattning

Finansinspektionen beslutar om 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. De nya reglerna träder i kraft den 1 juni 2014.

Syftet med föreskrifterna 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 nuvarande regler är få och generellt utformade. Det behövs därför mer precisa regler som ställer krav på företagen 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 informationssäkerhet, it-verksamhet och insättningssystem, innebär också att företag ska tillsätta resurser och genomföra åtgärder för att hantera riskerna.

Genom föreskrifterna 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 krav syftar till att slutligt anpassa den svenska regleringen till det så kallade insättningsgarantidirektivet.

Som en följd av de nya föreskrifterna inför Finansinspektionen även ändringar i Finansinspektionens föreskrifter (FFFS 2007:16) om värdepappersrörelse, som också börjar gälla den 1 juni 2014.

Innehåll

1 Utgångspunkter 3
1.1 Bakgrund 3
1.2 Målet med regleringen 4
1.3 Nuvarande och kommande regelverk 6
1.4 Ärendets beredning 7
1.5 Regleringsalternativ 7
1.6 Rättsliga förutsättningar 9
1.7 Ikraftträdandebestämmelser 10
2 Motivering och överväganden 10
2.1 Tillämpningsområde och definitioner 10
2.2 Proportionalitet 13
2.3 Allmänna råd 14
3 Nya föreskrifter och allmänna råd om hantering av operativa risker 15
3.1 Styrning och ansvar (2 kap.) 15
3.2 Identifiering och mätning (3 kap.) 17
3.3 Rapportering (4 kap.) 19
3.4 Hantering av operativa risker i verksamheten (5 kap.) 20
3.5 Ytterligare krav på hantering av operativa risker inom värdepappersrörelse och valutahandel (6 kap.) 31
4 Nya regler om informationssäkerhet, it-verksamhet, och insättningssyst ...36
4.1 Informationssäkerhet (2 kap.) 37
4.2 It-verksamhet (3 kap.) 43
4.3 Insättningssystem (4 kap.) 48
5. Följdändringar i andra föreskrifter och allmänna råd 52
5.1 Finansinspektionens föreskrifter (FFFS 2007:16) om värdepappersrörelse 52
5.2 Finansinspektionens allmänna råd (FFFS 2011:50) om ansökan om tillstånd att driva bank- eller finansieringsrörelse 53
6. Den nya regleringens konsekvenser 53
6.1 Allmänt om konsekvenser 53
6.2 Berörda företag 54
6.3 Konsekvenser för företagen och marknaden 54
6.4 Konsekvenser för samhället och konsumenten 60
6.5 Konsekvenser för Finansinspektionen 61

1 Utgångspunkter

1.1 Bakgrund

I ett företag 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. Dessa inre och yttre omständigheter utgör företagens operativa risker.[1]

Operativa risker finns i alla typer av verksamheter, men arten och omfattningen av riskerna 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).[2] De finansiella företagens verksamhetsmodeller utvecklas snabbt, vilket medför ständigt tillkommande källor till operativa risker. Exempel på en sådan utveckling är den snabbt växande trenden med utläggning av verksamhet till andra företag, vilket ofta sker i flera led och över landsgränser, så kallad outsourcing.

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. Eftersom

[1] Med operativ risk avses i dessa föreskrifter detsamma som i artikel 4.1 i Europaparlamentets 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 (CRR) risken för förluster till följd av ej ändamålsenliga eller fallerande processer, människor, system eller yttre händelser, inbegripet legala risker.

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

finansiella företag hanterar stora ekonomiska värden och känslig information är de 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 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 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 samt 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 gjorde Internationella valutafonden (IMF) en utvärdering av den finansiella sektorn i Sverige. I slutrapporten konstaterade IMF att Sverige saknar riktlinjer för hanteringen av operativa risker och rekommenderade att en sådan reglering tas fram.[3]

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

När det 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.[4] 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 redogörs för två nya föreskrifter som behandlar hur kreditinstitut, det vill säga banker och kreditmarknadsföretag, och

[3] "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.

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

värdepappersbolag ska arbeta med operativa risker. Den ena, föreskrifter och allmänna råd om hantering av operativa risker (nedan föreskrifterna om hantering av operativa risker), anger allmänna krav på företagen om hantering av operativa risker samt ytterligare krav inom värdepappersrörelse och valutahandel. Den andra, föreskrifter och allmänna råd om informationssäkerhet, it-verksamhet och insättningssystem (nedan föreskrifterna om informationssäkerhet, it-verksamhet och insättningssystem), reglerar hur företagen ska arbeta med informationssäkerhet, it-verksamhet och med 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 även Joint Forums[5] High-level principles for business continuity. Dessutom införs Europeiska banktillsynskommitténs (Cebs)[6] Guidelines on the management of operational risks in market-related activities. I och med detta 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 informationssäkerhet, it-verksamhet och insättningssystem inför Finansinspektionen regler som syftar till att begränsa de operativa riskerna när det gäller företagens informationshantering och it-system, 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 informationssäkerhet och it-system sedan lång tid tillbaka i de övriga nordiska länderna. Reglerna om insättningssystem syftar ytterst till att genomföra ändringarna i insättningsgarantidirektivet.[7]

---

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

[6] Europeiska banktillsynsfunktionen är sedan 2011 ersatt av 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).

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). Regler om värdepappersbolagens verksamhet finns i huvudsak i lagen (2007:528) om värdepappersmarknaden (LV). De kreditinstitut som har tillstånd att driva värdepappersrörelse ska även följa vissa bestämmelser i LV.

Organisatoriska krav för värdepappersbolag finns i Finansinspektionens föreskrifter (FFFS 2007:16) om värdepappersrörelse (värdepappersföreskrifterna). 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 krav på 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 för 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 Nya och kommande regler

I föreskriftsarbetet har hänsyn tagits till Finansinspektionens föreskrifter och allmänna råd (FFFS 2014:1) om styrning, riskhantering och kontroll i kreditinstitut (nedan föreskrifter om styrning, riskhantering och kontroll) som trädde i kraft den 1 april 2014.

Finansinspektionen har även beaktat den internationella regelutvecklingen på området, främst arbetet inom EU med det nya kapitaltäckningsdirektivet (CRD 4)[9] och kapitaltäckningsförordningen (CRR). Det är till exempel från artikel 85 i CRD 4 som kravet på att ett företag ska tillämpa interna regler och processer

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

[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.

för att utvärdera och hantera exponeringen för operativa risker kan härledas. Av samma artikel följer också att ett företag ska ha beredskaps- och kontinuitetsplaner för att säkerställa förmågan att löpande driva sin verksamhet och begränsa förlusterna vid en allvarlig störning i verksamheten.

1.4 Ärendets beredning

Finansinspektionen har i föreskriftsarbetet konsulterat och haft flera möten med en extern referensgrupp bestående av representanter från Svenska Bankföreningen, Finansbolagens Förening, Svenska Fondhandlareföreningen och Sparbankernas Riksförbund. Vidare har Finansinspektionen i fråga om vissa delar i föreskrifterna rådgjort med Myndigheten för samhällsskydd och beredskap (MSB), Riksbanken, Riksgälden och Datainspektionen.

Förslaget till förskrifter och allmänna råd skickades på remiss den 25 november 2013. Det presenterades i en remisspromemoria, och följande tre regelförslag bifogades: förslag till nya föreskrifter och allmänna råd om operativa risker, förslag till nya föreskrifter och allmänna råd om informationssäkerhet, it-verksamhet och insättningssystem, samt förslag till ändringar i värdepappersföreskrifterna. Under remisstiden höll Finansinspektionen ett öppet remissmöte med representanter från branschen och andra intressenter. Skriftliga synpunkter på förslaget har kommit in från Svenska Bankföreningen, Svenska Fondhandlareföreningen, Sparbankernas Riksförbund, Sveriges Advokatsamfund, Riksbanken, Riksgälden, Pensionsmyndigheten, Näringslivets regelnämnd, Datainspektionen, MSB, Regelrådet samt FAR, branschorganisationen för auktoriserade redovisningskonsulter, revisorer och rådgivare. Finansinspektionen har efter remitteringen bearbetat föreskriftförslagen och i arbetet beaktat remissinstansernas synpunkter.

De mest väsentliga synpunkterna redovisas och bemöts under respektive avsnitt. Föreskrifterna har även bearbetats redaktionellt.

1.5 Regleringsalternativ

Finansinspektionen har övervägt andra möjligheter för att säkra 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.

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.[10] 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.

Ett alternativ till att ge ut nya föreskrifter är att överlåta till branschen att själva reglera området, och i stället komplettera med vägledningar från Finansinspektionen. Skillnaderna mellan företagen är dock så stora att Finansinspektionen bedömer att det är svårt att uppnå en sådan samsyn att självreglering blir effektivt. Om det inte finns bindande regler på en ändamålsenlig detaljnivå är risken att utrymmet för tolkningar blir alltför stort, vilket försvårar för företagen att tillämpa reglerna och för Finansinspektionen att utöva tillsyn och föra dialog med företagen. Ytterst är det samhället och konsumenterna som får bära kostnaderna när riskhanteringen inte fungerar tillfredställande.

Hanteringen av operativa risker liksom hanteringen av andra risker, kostar pengar för företagen. Problemet ur samhällsekonomisk synpunkt är att kostnader som uppstår till följd av en störning i stor utsträckning spiller över på andra aktörer än den som orsakat störningen. Den typen av så kallade externa effekter leder erfarenhetsmässigt till att företag inte investerar i riskhantering på det sätt som är samhällsekonomiskt önskvärt. Operativa risker som omvandlas i inträffade incidenter kan medföra betydande kostnader för både företag, konsumenter och samhället. Finansinspektionen återkommer till detta i den konsekvensutredning som finns i avsnitt 6. 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 hos 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 därför 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 de krav som Riksgälden har på informationens tillförlitlighet och fullständighet. Finansinspektionen anser det därför nödvändigt att införa bindande regler om

[10] Se avsnitt 1.3 i beslutspromemorian Nya regler om styrning riskhantering och kontroll i kreditinstitut (FI dnr 11-5610).

insättningssystem. Det är dessutom nödvändigt för att fullständigt genomföra ändringarna i insättningsgarantidirektivet.

1.6 Rättsliga förutsättningar

Finansinspektionen får utfärda föreskrifter om vilka åtgärder ett kreditinstitut ska vidta för att bl.a. uppfylla kraven på riskhantering, genomlysning och sundhet i 6 kap. LBF med stöd av bemyndigandet i 16 kap. 1 § 3 LBF och 5 kap. 2 § 4 förordningen (2004:329) om bank- och finansieringsrörelse. I fråga om värdepappersbolag gäller bemyndiganden i 8 kap. 42 § 3–6 LV och 6 kap. 1 § 9–13, 29 förordningen (2007:572) om värdepappersmarknaden.

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

1.7 Ikraftträdandebestämmelser

Finansinspektionens ställningstagande: De nya föreskrifterna träder i kraft den 1 juni 2014.

Remissförslaget: Innehöll förslag om att föreskrifterna skulle träda i kraft den 1 maj 2014.

Remissinstanserna: *Svenska Bankföreningen, Svenska Fondhandlareföreningen, Sparbankernas Riksförbund* och *Finansbolagens Förening* påpekar att förslaget inte innehåller några övergångsbestämmelser och att det är nödvändigt att företagen får tid på sig att uppfylla de krav som föreskrifterna ställer. Bankföreningen och Fondhandlareföreningen anser att en övergångsperiod på minst 12 månader är nödvändig.

Finansinspektionens skäl: Finansinspektionen anser inte att det finns skäl för några generella övergångsbestämmelser eller en längre tid innan ikraftträdandet.

2 Motivering och överväganden

2.1 Tillämpningsområde och definitioner

2.1.1 Vilka företag omfattas och varför

Finansinspektionens ställningstagande: De nya föreskrifterna och allmänna råden gäller för kreditinstitut, det vill säga banker och kreditmarknadsföretag, samt värdepappersbolag. I dag innebär det att reglerna träffar totalt 259 företag under Finansinspektionens tillsyn. Av dessa är 89 banker, 45 kreditmarknadsföretag och 125 värdepappersbolag.

Kap. 6 föreskrifterna och allmänna råden om hantering av operativa risker, som handlar om ytterligare krav på hantering av operativa risker inom värdepappersrörelse och valutahandel, gäller för de företag som har tillstånd till investeringstjänster och investeringsverksamheter enlighet med 2 kap. 1 § 2–3 LV. Det handlar om omkring 90 företag som har något eller båda av dessa tillstånd. Det innebär att kapitlet, förutom värdepappersbolag med dessa tillståndstyper, även gäller för kreditinstitut med dessa tillstånd. De kreditinstitut som driver valutahandel med stöd av 7 kap. 1 § 12 LBF, ska också tillämpa reglerna.

Föreskrifterna om hantering av operativa risker inför i viss omfattning bestämmelser motsvarande de som redan gäller för värdepappersbolag i värdepappersföreskrifterna. För att inte värdepappersbolagen ska omfattas av två olika regelverk med samma innehåll, har Finansinspektionen, undantagit värdepappersbolagen från vissa av bestämmelserna i föreskrifterna om hantering av operativa risker. De bestämmelser som är undantagna framgår av

1 kap. 3 § föreskrifterna om hantering av operativa risker. Dessa bestämmelser motsvaras av bestämmelserna i 6 kap. 3 § och 21 kap. 2 § värdepappersföreskrifterna. Kreditinstitut med tillstånd att driva värdepappersrörelse ska dock tillämpa hela föreskriften även för värdepappersrörelsen.[11]

Det fjärde kapitlet i föreskrifterna om informationssäkerhet, it-verksamhet och insättningssystem, som handlar om insättningssystem, ska endast tillämpas av de företag som tar emot eller avser att ta emot medel som omfattas av insättningsgarantin.

Remisspromemorian: Förslaget hade i huvudsak samma innehåll, förutom att kap. 6 föreskrifterna om hantering av operativa risker avsågs gälla för fler tillståndstyper, det vill säga förutom 2 kap. 1 § 2–3 LV, även för punkterna 1 och 4 samma paragraf.

Remissinstanserna: *Finansbolagens Förening* anger att en tvingande reglering som främst riktar sig till banker och värdepappersbolag inte i alla delar är anpassade eller lämpade för alla kreditmarknadsbolag och anger även att det också är främst avseende de systemviktiga instituten som systemstabilitets- och skyddsargumenten är relevanta. *Svenska Bankföreningen* och *Svenska Fondhandlareföreningen* anser att de företag som ska omfattas av kap. 6 om ytterligare krav på hantering av operativa risker inom värdepappersrörelse och valutahandel bör begränsas till att enbart avse de företag som har tillstånd till utförande av order avseende finansiella instrument på kunders uppdrag samt handel med finansiella instrument för egen räkning, det vill säga 2 kap. 1 § 2–3 LV.

Finansinspektionens skäl: Finansinspektionen anser inte att det finns möjlighet att undanta vissa kreditmarknadsbolag från föreskrifterna. Finansinspektionen ser inte hur en sådan avgränsning av företag rent praktiskt skulle gå till, det vill säga vilken verksamhet som skulle anses vara så avgränsad eller vilka produkter vara så okomplicerade att de inte behöver omfattas av föreskrifterna. Finansinspektionen anser dock att, utöver verksamheter med valutahandel, 6 kap. föreskrifterna om operativa risker kan begränsas till att endast gälla de företag som har tillstånd enligt 2 kap. 1 § 2–3 LV, i enlighet med föreningarnas synpunkter. Syftet med bestämmelserna bedöms kunna uppnås trots denna inskränkning.

2.1.2 Definitioner

Finansinspektionens ställningstagande: Finansinspektionen behåller flertalet definitioner i föreskrifterna. Därutöver förtydligas definitionerna av beredskapsplan, kontinuitetsplan och återställningsplan. Med beredskapsplan

[11] Jämför avsnitt 2.4.1 i beslutspromemorian Nya regler om styrning riskhantering och kontroll i kreditinstitut (FI dnr 11-5610).

avses en plan som beskriver de åtgärder som ett företag ska vidta för att hantera allvarliga störningar, kriser och undantagstillstånd, som orsakas av till exempel omfattande avbrott i it-system, naturkatastrofer och dataintrång. Med kontinuitetsplan menas en plan som beskriver hur en verksamhet ska upprätthållas i händelse av ett avbrott eller en större verksamhetsstörning, till exempel genom tillgång till alternativ lokal eller utrustning. Med återställningsplan avses en plan som beskriver vilka prioriteringar och rutiner ett företag ska ha för att återgå till normal verksamhet efter ett avbrott eller en större verksamhetsstörning.

Remisspromemorian: Förslaget hade i huvudsak samma innehåll.

Remissinstanserna: *Svenska Bankföreningen* och *Svenska Fondhandlareföreningen* anför att definitionen av beredskapsplan, kontinuitetsplan och återställningsplan är snarlika och att det är oklart vad det bakomliggande syftet är med att dela upp dessa begrepp. Föreningarna framför även att definitionerna bör omarbetas så att det tydligt framgår att de olika planerna kan samlas i ett gemensamt dokument. *Sparbankernas Riksförbund* framför i stort sett samma synpunkter. *Finansbolagens förening* anger i sitt remissvar att det i definitionen av incident bör läggas till ett väsentlighetskrav.

Finansinspektionens skäl: Begreppen beredskapsplan, kontinuitetsplan och återställningsplan återfinns i GL 44 och används på samma sätt i dessa föreskrifter. Finansinspektionen anser inte att det finns ett behov av att ändra i uppdelningen av dessa. Det finns dock inget hinder för ett företag att ge de interna dokumenten andra namn än just beredskapsplan, kontinuitetsplan och återställningsplan så länge som de uppfyller kraven i föreskrifterna. Syftet med planerna är att säkerställa att ett företag har förmågan att hantera olika typer av avbrott och störningar. Medan man vanligtvis i den dagliga verksamheten kan hantera mindre avbrott och störningar behövs det ett planlagt arbetssätt för att hantera extraordinära omständigheter som kan påverka många kunder, andra företag eller leverantörer, men även stora delar av personalen. En beredskapsplan fokuserar på förberedelser för ledning och hantering av omfattande avbrott och störningar i verksamheten. En kontinuitetsplan innehåller vanligtvis en beskrivning av reservrutiner, tillgång till alternativa lokaler och utrustning som möjliggör fortsatt verksamhet när ordinarie rutiner, lokaler eller utrustning inte fungerar. Syftet med den tredje typen av plan, återställningsplanen, är att i förväg fastställa prioriteringar och rutiner för hur verksamheten (både när det gäller verksamhetsprocesser och it-system) ska återgå till normala rutiner efter avbrott eller störning. Definitionerna av vad som avses med respektive plan har omarbetas något för att tydliggöra kravet på de olika planerna, se även avsnitt 3.4.7.

Finansinspektionen anser inte att ett väsentlighetskriterium ska införas i definitionen av incident. Incidenter som var för sig inte uppnår väsentlighetskriteriet skulle därmed inte tas omhand i riskhanteringen. Flera sådana incidenter kan dock sammantaget ha betydande inverkan på ett företags verksamhet. Dessutom för ett sådant kriterium med sig subjektiva bedömningar

som skapar svårigheter i tillämpningen för företagen och i tillsynen för Finansinspektionen.

2.1.3 Tillämpning av reglerna på finansiell företagsgrupp.

Finansinspektionens ställningstagande: Föreskrifterna ska inte tillämpas på finansiella företagsgrupper. Finansinspektionen avser dock att införa sådana bestämmelser inom kort.

Remisspromemorian: Förslaget hade samma innehåll.

Remissinstanserna: Remissinstanserna har inte lämnat några synpunkter.

Finansinspektionens skäl: Den 1 januari 2014 trädde CRR i kraft. Det pågår för närvarande ett regelarbete för att genomföra CRD 4 i Sverige. Reglerna förväntas i viss mån ändra innebörden av begreppet finansiell företagsgrupp och hur det ska hanteras i riskhänseende.

2.2 Proportionalitet

Finansinspektionens ställningstagande: Proportionalitetsprincipen gäller om det anges särskilt i föreskrifterna. Principen gäller även i den mån det följer av tillämpliga bestämmelser enligt lag.

Remisspromemorian: Förslaget hade samma innehåll**.**

Remissinstanserna: *Svenska Bankföreningen* och *Svenska Fondhandlareföreningen* anför att proportionalitetsprincipen följer av lag och bör tillämpas i fråga om de krav som ställs i föreskrifterna. Föreningarna ifrågasätter om det är förenligt med lagens krav att Finansinspektionen i remissförslaget inför denna princip endast på vissa klart avgränsade områden. *Sparbankernas Riksförbund* framför liknande synpunkter. *Advokatsamfundet* och *Finansbolagens Förening* anser att en generell bestämmelse om proportionalitet bör införas i föreskrifterna.

Finansinspektionens skäl: Vid all rättstillämpning gäller en proportionalitetsprincip, det följer av såväl gemenskapsrätten som av svensk rätt, som bland annat innebär att ingripanden inte ska gå utöver vad som behövs med hänsyn till ändamålet. Även utformningen av författningar är underkastad en proportionalitetsbedömning och det är den som diskuteras här.

Av förarbetena till 6 kap. LBF och 8 kap. LV framgår att de krav som ställs på instituten enligt bestämmelserna om soliditet och likviditet, riskhantering och genomlysning kan variera med de verksamheter instituten ägnar sig åt.[12] Bestämmelserna i 6 kap. 1–3 §§ LBF ska enligt 6 kap. 4 a § samma lag

[12] Prop. 2002/03:39 s. 275, 277 och 279 f. och prop. 2006/2007:215.

omfattas av proportionalitet och enligt förarbetena till denna bestämmelse framgår det att Finansinspektionen bör beakta proportionalitetsprincipen när den utformar föreskrifter. Det är alltså fråga om proportionalitet vid regelgivning. Finansinspektionen har i arbetet med de nya föreskrifterna beaktat proportionalitetsprincipen och har bedömt att det i vissa fall kan klargöras att principen medger olika krav på olika företag.

Exempel på bestämmelser som kan omfattas av proportionalitet är 3 kap. 1 § föreskrifterna om hantering av operativa risker om krav på metoder för att mäta och identifiera operativa risker eller 3 kap. 7 § förskrifterna om informationssäkerhet, it-verksamhet och insättningssystem om fastställande av interna regler för informationssäkerhet. Det innebär dock inte till exempel att små företag som driver mindre komplex verksamhet helt ska befrias från att tillämpa bestämmelserna, utan att företagen utifrån verksamhetens art, omfattning och komplexitet ska anpassa sig till kraven.

Ett företags storlek kan bestämmas utifrån en samlad bedömning av olika kriterier såsom balansomslutning, storlek på kapitalbasen, marknadsandelar av olika verksamhetsgrenar, antalet anställda, associationsform och om företagets aktier är upptagna till handel osv. I bedömningen av verksamheters art, omfattning och komplexitet bör företaget ta hänsyn till de olika tillstånd det har (till exempel tillstånd att använda interna metoder för beräkning av kapitalkrav), de faktiska verksamheter företaget driver (såsom kreditgivning och omfattande egen handel) samt komplexiteten i de produkter som tillhandahålls.

2.3 Allmänna råd

Finansinspektionens ställningstagande: Föreskrifterna ska inte innehålla allmänna råd som också finns som riktlinjer i GL 44. De allmänna råd i föreskrifterna som inte finns i GL 44, men som kan finnas i andra vägledningsdokument, behålls.

Remissförslaget: Förslaget hade i huvudsak samma innehåll. Förslaget om operativa risker innehöll dock allmänna råd med ursprung från både GL 44, andra vägledningsdokument och erfarenheter från Finansinspektionens tillsyn.

Remissinstanserna: *Svenska Bankföreningen* och *Svenska Fondhandlareföreningen* anför att de exempel och förtydliganden till föreskrifttexterna som anges som allmänna råd i föreskrifterna i stället bör ges i remisspromemorian. Föreningarna anser att en sammanblandning av krav och råd inte ökar tydligheten utan i stället skapar oklarhet. Föreningarna anser även att det är oklart hur GL 44:s rekommendationer förhåller sig till de allmänna råden i föreskrifterna om operativa risker.

Finansinspektionens skäl: Finansinspektionens beslutspromemorior är inte en rättskälla. När Finansinspektionen vill lämna företagen vägledning om hur en viss bestämmelse i en föreskrift kan följas görs detta genom allmänna råd i

anslutning till bestämmelsen i föreskriften. För att undvika dubbelreglering tar Finansinspektionen bort de allmänna råd som har samma innebörd som riktlinjerna i GL 44. Företagen ska alltså följa riktlinjerna i GL 44 i alla delar som Finansinspektionen inte anser att det behövs en tvingande bestämmelse. Övriga allmänna råd lämnas oförändrade i föreskriftstexten.

3 Nya föreskrifter och allmänna råd om hantering av operativa risker

I detta avsnitt redogör Finansinspektionen för överväganden och ställningstaganden som gjorts i arbetet med att ta fram de nya föreskrifterna. Redogörelsen följer samma ordning som kapitlen i 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
- ytterligare krav på hantering av operativa risker inom värdepappersrörelse och valutahandel (6 kap.).

3.1 Styrning och ansvar (2 kap.)

Finansinspektionens ställningstagande: Ett företag ska ha en fastställd riskaptit och fastställda limiter för operativa risker. Limiterna ska tas fram inom ramen för riskaptiten. De ska vara mätbara genom kvantitativa eller kvalitativa mått, och företaget ska utgå från produkter, tjänster, funktioner, processer och it-system när det fastställer limiterna. Riskaptiten ska beslutas av företagets styrelse och limiterna av företagets verkställande direktör. Ett företag ska också ha interna regler för hantering av operativa risker. Dessa regler ska beslutas av företagets styrelse.

Remisspromemorian: Förslaget hade i huvudsak samma innehåll. I förslaget saknades krav på riskaptit för operativa risker och begreppet risktolerans användes i stället för limiter.

Remissinstanserna: *Riksgälden* anser att Finansinspektionen utöver begreppet risktolerans bör införa begreppet riskaptit i den övergripande styrningen av operativa risker. Riksgälden påpekar att riskaptit och risktolerans enligt bland annat Committee of Sponsoring Organizations of the Treadway Commission (COSO) är två olika begrepp som båda bör vara dokumenterade och fastställda av ett företags styrelse.

Finansbolagens Förening anser att periodiciteten av utvärdering av risktoleransen behöver anges, exempelvis en gång per år, och att uppdatering bör ske vid behov. Föreningen framhåller även vikten av att kraven på att

styrelsen beslutar om interna regler för hantering av operativa risker bör stämmas av och samordnas med den aktiebolagsrättsliga regleringen.

När det gäller interna regler för hantering av operativa risker anser *Svenska Bankföreningen* att begreppet risköverföring bör tas bort eller att det bör förtydligas och inkludera en väsentlighetsprincip.

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

Finansinspektionen instämmer med Riksgäldens synpunkt att begreppet riskaptit bör användas i den övergripande styrningen av operativa risker. I motiveringen till införande av föreskrifterna om styrning, riskhantering och kontroll (s. 17–19) förs ett längre resonemang kring de båda begreppen, och i dessa föreskrifter har inspektionen valt att enbart använda riskaptit som begrepp för en accepterad nivå och inriktning på företagets risker. Finansinspektionen anser inte när det när gäller reglerna om operativa risker att det finns anledning att göra ett annat ställningstagande.

Ett företags hantering av sina operativa risker kan på både kort och lång sikt påverka företagets överlevnad. Beslut om nivån och inriktningen på riskerna är inte lämpliga att placera på ett annat bolagsorgan än företagets styrelse (se även diskussionen om styrelse och verkställande direktörs ansvar och uppgifter i motiveringen till införande av föreskrifterna om styrning, riskhantering och kontroll [s. 28 ff.]). Genom en sådan ordning skapas grundläggande förutsättningar för att riskhanteringen får det fokus som krävs i organisationen. Det är också rimligt att styrelsen fastställer de interna reglerna för hantering av operativa risker. Kravet på att styrelsen ska besluta dessa interna regler innebär att den inte kan delegera uppgiften att besluta om dessa till någon annan.

I fråga om att fastställa limiter gör Finansinspektionen ett förtydligande gentemot det remitterade förslaget. Limiter ska tas fram för produkter, tjänster, funktioner, processer *och* it-system, i stället för *eller*. Därmed bör det vara tydligt att företaget ska beakta alla dessa dimensioner. Limiter bör bestämmas på en sådan nivå att det är möjligt för företaget att använda limiterna i sin kontroll och styrning av operativa risker.

Finansbolagens Förening anser att periodiciteten för utvärdering av riskaptiten ska anges i föreskrifterna. Finansinspektionen håller inte med och anser att hur ofta detta ska göras bör bestämmas efter det enskilda företagets förutsättningar. För vissa företag, som inte genomför några större ändringar i sina produkter, processer eller it-system kan en gång per år eller till och med mer sällan vara tillräckligt. Stora och komplexa företag eller företag som genomför större förändringar i till exempel sin organisation eller i it-system kan behöva göra mer frekventa utvärderingar och uppdateringar. Finansinspektionen lämnar därför till företagen att avgöra hur ofta utvärdering bör göras. Däremot håller Finansinspektionen med Finansbolagens Förening att uppdatering bör ske om

det behövs och inte regelbundet. En regel med denna innebörd införs i föreskriften.

Eftersom verksamheter kan ha olika komplexitet och omfattning inför Finansinspektionen en proportionalitetsregel 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.

Finansinspektionen håller med Bankföreningen om att begreppet risköverföring behöver tydliggöras och gör ett tillägg om att det handlar om risköverföring inom ramen för hantering av operativa risker och inte inom ramen för kapitalberäkning enligt internmätningsmetoden.

3.2 Identifiering och mätning (3 kap.)

Finansinspektionens ställningstagande: Ett företag ska identifiera operativa risker i sina produkter, tjänster, funktioner, processer och it-system. Företaget ska regelbundet mäta riskerna genom att bedöma sannolikheten för att de inträffar och dess konsekvenser. Metoderna för identifiering och mätning ska vara dokumenterade. För att få en förvarning om ökade risker ska ett företag ha indikatorer och gränsvärden. Företaget ska ha interna regler för att hantera incidenter. Incidenter ska dokumenteras och analyseras.

Remisspromemorian: Förslaget hade i huvudsak samma innehåll. Förslaget innehöll dock en precisering av olika typer av åtgärder som skulle vidtas för att hantera de operativa riskerna. Denna precisering tas bort. De allmänna råden gällande indikatorer kunde till följd av ordet ”eller” uppfattas som alternativa. Det ändras till ”och”. I förslaget fanns inte heller bestämmelsen som undantar kravet på dokumentation och analys i fråga om incidenter som anmäls anonymt. Kravet på inhämtning av information om incidenter och förluster vid utläggning av verksamhet tas bort.

Remissinstanserna: *Svenska Bankföreningen, Svenska Fondhandlareförening* och *Finansbolagens Förening* anser att formuleringen i remissförslaget att ”[e]tt företag ska identifiera operativa risker i sina produkter, tjänster, funktioner, processer och it-system” bör ändras till ”[e]tt företag ska identifiera operativa risker i sin verksamhet”. Den senare formuleringen ger företagen bättre möjlighet att anpassa identifieringen av operativa risker till respektive företags verksamhet och fokusera på området som it, anläggningar eller leverantörer. Likaså anser Bankföreningen och Fondhandlareföreningen att bestämmelsen om riskindikatorer bör ändras till att ”[e]tt företag ska fastställa *egna* indikatorer och gränsvärden för sina operativa risker som ger en indikation på att risken ökar”. Föreningarna påtalar även att det är viktigt med övergångsbestämmelser för att ge företagen en rimlig möjlighet att införa meningsfulla riskindikatorer. Beträffande bestämmelserna om incidenter menar

samtliga tre föreningar att ett väsentlighetskrav bör införas så att dokumentation och analys endast gäller incidenter som kan få en reell negativ påverkan på företaget.

Bankföreningen och Fondhandlareföreningen anser att bestämmelsen om utläggning av verksamhet innebär en dubbelreglering mot bestämmelserna om incidenter, eftersom incidenter ska hanteras i alla delar av verksamheter oavsett om de är utlagda eller inte.

Myndigheten för samhällsskydd och beredskap (MSB) anser däremot att det i bestämmelsen om utläggning av verksamhet ska införas krav på att ett företag säkerställer att information om incidenter och förluster omgående rapporteras av uppdragstagaren till företaget.

Riksgälden välkomnar att Finansinspektionen föreskriver om incidenter men anser att kravet på att ett företag ska säkerställa att uppgifter om incidenter och förluster är korrekta bör nyanseras, så att det detta krav inte hindrar att incidenter kan rapporteras in anonymt.

Finansinspektionens skäl: 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 strukturerat 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. Den regel som föreskriver om identifiering av riskerna behöver därför också ha en viss mån av detaljnivå. Finansinspektionen bedömer att det är lämpligt att precisera att det är viktigt att identifiera risker i produkter, tjänster, funktioner, processer och it-system. Finansinspektionen instämmer med remissinstanserna att det kan finnas andra viktiga områden med operativa risker, som till exempel anläggningar och leverantörer. Den regel som nu införs hindrar inte företagen från att beakta dessa områden.

Kraven på mätning av operativa risker innebär inte att ett företag nödvändigtvis ska utveckla egna kvantitativa beräkningsmodeller. Syftet med regeln är att företaget ska ha kriterier och mått som det tillämpar systematiskt. Företaget kan därför välja om det vill tillämpa kvantitativa eller kvalitativa mått. Det väsentliga är att företaget är konsekvent vid mätningen av de operativa riskerna. Det ger företaget en möjlighet att följa hur riskerna utvecklas över tid.

Finansinspektionen bedömer inte att det tillför regeln något genom tillägget ”egna” indikatorer. Det centrala är att indikatorerna kan tillämpas på företagets operativa risker. Till regeln om riskindikatorer 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. Genom kravet på att ett företag ska analysera och dokumentera uppgifter om de incidenter och de förluster som har uppstått i samband med dessa, 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. Finansinspektionen har övervägt att införa ett väsentlighetskrav för analys och dokumentation av incidenter i enlighet med föreningarnas förslag, men anser att införande av ett sådant krav skulle skapa både svårigheter i tillämpningen för företagen och i tillsynen för Finansinspektionen. Med ett väsentlighetskrav finns risk för att incidenter som är en viktig källa till kunskap om operativa risker inte dokumenteras och analyseras när företaget inte anser att incidenterna är väsentliga. Informationen kommer då inte användas i riskhanteringen. Finansinspektionen beaktar Riksgäldens förslag om att undanta incidenter som anmäls anonymt från kravet på rutiner för att säkerställa att uppgifter om incidenter och förluster är korrekta.

Som tidigare nämnts i denna promemoria finns i dag en snabbt växande trend med utläggning av verksamhet till andra företag, så kallad outsourcing. Utgångspunkten är att det alltjämt är det uppdragsgivande företaget som ansvarar för riskerna och riskhanteringen i verksamheten även om den 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. Finansinspektionen delar Bankföreningens och Fondhandlareföreningens synpunkt att bestämmelsen om utläggning av uppdragsavtal innebär en dubbelreglering. Kravet i bestämmelsen om uppdragsavtal om inhämtning av information från uppdragstagare tas därför bort.

I fråga om de synpunkter som förts fram om ett senare ikraftträdande, se avsnitt 1.7.

3.3 Rapportering (4 kap.)

Finansinspektionens ställningstagande: Ett företag ska i sin rapportering av operativa risker till styrelsen och verkställande direktören ange indikatorer för operativa risker. Styrelsen och den verkställande direktören ska också få information om överträdelser av riskaptit och risklimiter samt om allvarliga incidenter. Minst årligen ska styrelsen informeras om resultatet från tester av beredskapsplaner, kontinuitetsplaner och återställningsplaner.

Remisspromemorian: Förslaget hade i huvudsak samma innehåll. Risktolerans ersätts dock med riskaptit och risklimiter.

Remissinstanserna: *Finansbolagens Förening* anser att Finansinspektionen bör införa en hänvisning i föreskriften till de generella krav på rapportering som finns i Finansinspektionens föreskrifter och allmänna råd om styrning, riskhantering och kontroll. *Svenska Bankföreningen* och *Svenska Fondhandlareförening* föreslår att texten gällande information till styrelsen om resultatet från tester av beredskapsplaner, kontinuitetsplaner och återställningsplaner ersätts av information till styrelsen om status för kontinuitetshantering, då det sistnämnda ger mer relevant information till styrelsen.

Finansinspektionens skäl: I sin tillsynsverksamhet 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 inför därför några grundläggande krav på den information som ska ingå i rapporteringen om operativa risker till styrelsen och den verkställande direktören. Dessa rapporteringskrav gäller utöver de krav som redan finns på rapportering av risker i 6 kap. värdepappersföreskrifterna och 5–8 kap. föreskrifterna om styrning, riskhantering och kontroll.

Finansinspektionen anser att det finns ett behov av konkreta krav på rapportering till styrelsen gällande tester av beredskapsplaner, kontinuitetsplaner och återställningsplaner. Effektiviteten i planerna är den mest grundläggande delen av kontinuitetshanteringen. Finansinspektionen håller därför inte med föreningarna om deras synpunkt om information till styrelsen.

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

3.4.1 Processer (5 kap. 1–4 §§)

Finansinspektionens ställningstagande: Ett företag ska fastställa och i en förteckning ange vilka processer i verksamheten som är av väsentlig betydelse. Företaget ska dokumentera processerna och utse en ansvarig person eller funktion för varje process. Processdokumentationen bör beskriva vilka regler som påverkat processens utformning, de huvudsakliga aktiviteterna i processen och deras samband, vilken information som används i processen och vilket krav på kvaliteten på informationen som ställs. Vidare bör processdokumentationen omfatta vilka it-system som stödjer processen, vilka kontroller som görs och vilka beslut som fattas, vilka som berörs av processen och vilket resultat som processen avser att ge upphov till. Ett företag ska också ha rutiner för att analysera om det finns aktiviteter i processerna som innebär

risk för betydande förluster på grund av till exempel misstag eller manipulering av information. Om sådana aktiviteter identifieras ska företaget införa nödvändiga kontroller i processerna.

Remisspromemorian: Förslaget hade i huvudsak samma innehåll. I förhållande till förslaget ändras dock bestämmelsen om uppdatering av förteckningen över processer från att uppdateringen ska ske ”regelbundet” till ”om det behövs”. Vidare ändras bestämmelsen om att det ska finnas en ansvarig person för varje process till en person eller funktion.

Remissinstanserna: *Svenska Bankföreningen* och *Svenska Fondhandlareföreningen* anser att bestämmelserna om processförteckning, processdokumentation, processansvarig och analys av processerna ska strykas. I varje fall behöver företagen en längre tid för genomförande av bestämmelsen. Visserligen håller föreningarna med om att processdokumentation kan vara till hjälp för att identifiera brister och risker, men de anser att mycket detaljerad kartläggning av processer, produkter och system sker på bekostnad av andra mer relevant riskmildrande åtgärder. Vidare utrycker Bankföreningen och Fondhandlareföreningen en oro över att föreskrifterna kan komma att resultera i att företagen inför en processbaserad verksamhetsmodell, då remissinstanserna uppfattar att processägarna kommer att få stärkt mandat.

Finansbolagens Förening anser att periodiciteten för uppdatering av processförteckningen ska anges. Rimligtvis ska detta ske årligen och inte regelbundet. Samtliga tre föreningar anser att Finansinspektionen bör tydliggöra ansvaret för processer av väsentlig betydelse och att ansvaret kan fullgöras även av en funktion.

Finansinspektionens skäl: 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 snarlikt förhållande.[13]

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.

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

Utifrån ett riskbaserat arbetssätt ställer Finansinspektionen endast krav på att företaget ska dokumentera de processer som är av väsentlig betydelse för företagets verksamhet. Ett företag ska därför fastställa vilka de processerna är och sedan dokumentera dem. 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. Genom att processerna dokumenteras bör riskerna i dem bli tydliggjorda och en effektiv hantering av dessa risker möjliggörs. Det skapar förutsättningar för en ändamålsenlig prioritering av resurser.

Bestämmelsen i 5 kap. 3 § omfattas av proportionalitet. 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 ett stort företag kan handla om ett stort antal processer där gemensamma standarder för dokumentation av processerna kan behöva utvecklas.

För att tydliggöra och hantera de operativa riskerna på ett systematiskt sätt anser Finansinspektionen att det måste finnas en dokumentation av processerna. Aktivitetskedjor som inte är dokumenterade ger inte möjlighet att på ett effektivt sätt kunna identifiera risker och brister. En allt för generell dokumentation ger enligt Finansinspektionens bedömning inte tillräckligt underlag för företaget att göra nödvändiga analyser och bedömningar, medan en allt för detaljerad dokumentation kan försvåra hanteringen av risker. Finansinspektionen håller med om att en mycket detaljerad kartläggning av processer, produkter och system kan ske på bekostnad av andra riskmildrande åtgärder. Därför anser Finansinspektionen att det är viktigt att varje företag anpassar dokumentationskravet till sina behov och förutsättningar. Genom de allmänna råden om processdokumentation skapas en tydlig nivå för vad en dokumentation bör innehålla. Det är inte Finansinspektionens avsikt att ge ut regler som gör att företagen inför en processbaserad verksamhetsmodell. Aktivitetskedjor finns i alla finansiella företag, de kan vara olika långa eller komplexa. Att dokumentera dessa motverkar å ena sidan en fragmenterad bild av aktiviteterna och personberoenden å andra sidan, tydliggörs ansvaret för olika aktiviteter och kartläggningen av nyckelkontroller underlättas. Eftersom aktivitetskedjor finns på alla företag, anser Finansinspektionen inte att det påverkar företagens verksamhetsmodeller eller styrmodeller.

Finansinspektionen ändrar kravet på företagets uppdatering av förteckningen över sina processer, från att den ska vara regelbunden till att den ska ske om det behövs.

Finansinspektionen tydliggör kravet på ansvar för en process utifrån remissinstansernas synpunkter. Det kan vara en person eller funktion som har det ansvaret. Då begreppet funktion, som finns definierad i föreskrifterna om styrning, riskhantering och kontroll är organisatoriska enheter, innebär ändringen inte någon förändring i sak.

I fråga om de synpunkter som förts fram om ett senare ikraftträdande, se avsnitt 1.7.

3.4.2 Personal (5 kap. 5 §)

Finansinspektionens ställningstagande: Ett företag ska ha rutiner för hur det hanterar operativa risker i fråga om sin personal, där det framgår hur företaget kontrollerar nödvändiga uppgifter i samband med att företaget anställer ny personal. Företaget ska särskilt beakta risken för intressekonflikter. Ett företag ska se till att det har tillräckligt med personal i förhållande till arbetsuppgifterna och utvärdera om det har personal med en sådan kompetens eller som fyller en sådan funktion att de är svåra att ersätta med kort varsel. Företaget ska i så fall utse ersättare för sådan personal. Vidare ska ett företag fastställa krav på kompetens och kunskap för sin personal samt se till att kompetensen och kunskapen upprätthålls. Företaget ska ha rutiner för fastställande och uppdatering av befattningsbeskrivningar, mandat och limiter samt för hur det hanterar den tystnadsplikt som regleras i 1 kap. 10 § LBF och 1 kap. 11 § LV. Det ska också finnas rutiner för hur företaget identifierar och hanterar operativa risker som kan uppstå i samband med att personalen internt byter arbetsuppgifter eller organisatorisk enhet.

Remisspromemorian: Förslaget hade i huvudsak samma innehåll. Förslaget innehöll dock bestämmelser om kontroll av viktiga uppgifter gällande befintlig personal, och om identifiering och hantering av risker som kan uppstå i samband med personalens ledighet.

Remissinstanserna: *Finansbolagens Förening* anser att bestämmelsen att företag ska ha rutiner för att identifiera och hantera operativa risker som kan uppstå i samband med personalens ledighet ska utgå. *Svenska Bankföreningen* och *Svenska Fondhandlareföreningen* har samma förslag med motivering att detta krav indirekt framgår av kraven på att ett företag ska ha tillräckligt med personal med rätt kompetens. Vidare anser Bankföreningen och Fondhandlareföreningen att det bör framgå av promemorian vilka uppgifter som ska kontrolleras vid nyanställning och vad som menas med ”befattningar som har särskild betydelse för företagets riskexponering”. Föreningarna anser även att bestämmelsen om sekretess kan strykas eftersom den regleras i rörelselagstiftningen.

Finansinspektionens skäl: 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. Det finns därför skäl att ha regler som hanterar operativa risker hänförliga till 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. Finansinspektionen kan inte i detalj ange vilka typer av uppgifter som ska kontrolleras eftersom detta beror på företagets verksamhet och vilken tjänst eller funktion som anställningen gäller.

Finansinspektionen anser dock att risken för intressekonflikter är något som särskilt ska beaktas redan vid nyanställning. Eftersom kraven på hantering av intressekonflikter i verksamheten finns i 4 kap. i förskrifterna om styrning, riskhantering och kontroll stryks andra delen av bestämmelsen om kontroller under anställningstiden.

Företag kan ha personal med kompetens som är svår att ersätta med kort varsel och som är nödvändig för företagets verksamhet. Det kan till exempel handla om personer med särskilda kunskaper om specifika it-system eller personer som dagligen utför viktiga kontroller. Ett företag behöver ta ställning till om den funktion som personen fyller behöver utföras även om personen är frånvarande och hur företaget i så fall säkerställer att det görs.

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. Därför införs krav på att ett företag ska vara skyldigt att ha rutiner om befattningsbeskrivningar, limiter och mandat.

Finansinspektionen delar remissinstansernas syn på att risker som kan uppstå i samband med personalens ledighet, till exempel som har att göra med bemanning och kompetens, tas omhand av kraven i 5 kap. 5 § 2–4 på att ett företag ska ha tillräckligt med personal i relation till arbetsuppgifterna och personal med rätt kompetens. Bestämmelsen i förslaget om identifiering och hantering av risker som kan uppstå i samband med personalens ledighet tas därför bort.

Finansinspektionen delar inte Bankföreningens och Fondhandlareföreningens syn på att bestämmelsen om tystnadsplikt är obehövlig. Syftet med bestämmelsen i föreskriften är att det ska finnas rutiner kring kravet i kap. 10 § LBF och 1 kap. 11 § LV.

Exempel på en ytterligare risk förknippad med personal är när en anställd byter befattning inom företaget. Det kan handla om att en anställd, som i sin tidigare roll har haft mandat att genomföra transaktioner som innebär 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. Därför ska ett företag ha rutiner för att identifiera och hantera de operativa risker som kan uppstå när personal internt byter arbetsuppgifter eller enheter.

3.4.3 Legala risker (5 kap. 6 §)

Finansinspektionens ställningstagande: Ett företag ska ha interna regler för hantering av legala risker. De interna reglerna ska ange på vilket sätt företaget säkerställer att verksamheten följer lagar, förordningar och andra regler som gäller för verksamheten. De interna reglerna ska också ange hur företaget säkerställer att ingångna avtal och andra rättshandlingar är korrekta och giltiga, hur avtal och andra rättshandlingar arkiveras samt hur rättsliga processer hanteras. Företaget ska ha en person eller funktion som ansvarar för detta.

Remisspromemorian: Förslaget hade i huvudsak samma innehåll. I förslaget fanns dock en definition av legal risk och att en organisatorisk enhet kunde utses som ansvarig för legala risker.

Remissinstanserna: *Finansbolagens Förening*, *Svenska Bankföreningen* och *Svenska Fondhandlareföreningen* anser att Finansinspektionen bör tydliggöra hur begreppet legala risker förhåller sig till regelefterlevnadsrisker.

Bankföreningen och Fondhandlareföreningen anser att grunder för den i föreskriftförslaget angivna definitionen av legal risk bör beröras i promemorian samt att Finansinspektionen bör ange vad som kan inbegripas i begreppet ”andra rättshandlingar”. Föreningarna anser att 5 kap. 7 § 3 bör strykas eller samordnas med kraven i 8 kap. föreskrifterna om styrning, riskhantering och kontroll. Vidare anser föreningarna att det ska framgå av regleringen att det är en funktion som kan ansvara för hantering av legala risker.

Finansinspektionens skäl: Tvister, brister i rättshandlingar och rättsliga dokument eller bristande regelefterlevnad kan orsaka höga förluster, omfattande ryktesproblem eller andra negativa konsekvenser för ett företag. Bestämmelserna om att ett företag ska ha interna regler för sin hantering av legala risker ska därför säkerställa att det finns ett strukturerat arbetssätt med dessa frågor i företaget.

Finansinspektionen har i arbetet med de nya föreskrifterna konstaterat att det finns olika definitioner av legal risk i olika källor. Finansinspektionen avstår dock från att definiera vad som menas med legal risk i dessa föreskrifter. De definitioner som Finansinspektionen har beaktat vid utformningen av bestämmelsen är dels definitionen av legal risk från Financial stability institute (FSI)[14], dels definitionen av operativ och legal risk i Baselkommitténs *International Convergence of Capital Measurementand Capital Standards A*

[14] Legal risk refers to the risk of unenforceable contracts (in whole or in part), lawsuits, adverse judgments or other legal proceedings disrupting or adversely affecting the operations or condition of a bank. It can arise due to a variety of issues, from broad legal or jurisdictional issues to something as simple as a missing provision in an otherwise valid agreement.

Revised Framework, juni 2006, punkt 644)[15], samt dels definitionen av regelefterlevnadsrisk i GL 44[16].

Finansinspektionen är medveten om att det i dag finns en viss överlappning mellan definitionerna av legal risk och regelefterlevnadsrisk.

Regelefterlevnadsrisk bör, enligt Finansinspektionens mening, betraktas som en typ av legal risk, snarare än helt ny typ av risk separerad från definitionen av legal risk. Detta baserar Finansinspektionen på att regelefterlevnadsrisker vanligtvis orsakas av samma grundorsaker som andra typer av legala risker, till exempel bristande kompetens, felaktiga rutiner eller ineffektiva kontroller.

I 8 kap. föreskrifterna om styrning riskhantering och kontroll finns bestämmelser med krav dels på identifiering och hantering av regelefterlevnadsrisker, dels ansvarsområdet för funktionen för regelefterlevnad.

I sista stycket förtydligar Finansinspektionen att det kan vara en person eller en funktion som ska ansvara för hanteringen av legala risker.

3.4.4 Säkerhetsarbete (5 kap. 7–8 §§)

Finansinspektionens ställningstagande: Ett företag ska ha interna regler för säkerhetsarbete och i dessa fastställa vilka tillgångar och värden som ska skyddas. Företaget ska ange vilka åtgärder det ska vidta för att skydda dessa och hur omfattande åtgärderna ska vara. Denna bestämmelse kompletteras med allmänna råd att företaget bör använda scenarion eller simuleringar för att öka kunskapen om hur olika typer av hot, oegentligheter och brottsliga handlingar kan uppstå i företagets verksamhet.

Remisspromemorian: Förslaget hade i huvudsak samma innehåll.

Remissinstanserna: *Svenska Bankföreningen* och *Svenska Fondhandlareföreningen* anser att meningen ”när sådana händelser inträffar” bör tas bort från de allmänna råden Detta då det bör hanteras inom ramen för incidenthanteringen och därmed blir meningen överflödig. Vidare anser

[15] Operational risk is defined as the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. This definition includes legal risk, but excludes strategic and reputational risk. Legal risk includes, but is not limited to, exposure to fines, penalties, or punitive damages resulting from supervisory actions, as well as private settlements.

[16] I GL 44 definieras regelefterlevnadsrisk som den aktuella eller potentiella risken för påverkan på intäkter och kapital som uppstår till följd av överträdelser eller bristande efterlevnad av lagar, bestämmelser, avtal, föreskrivna rutiner eller etiska standarder. Sådana risker kan leda till böter, skadestånd och/eller annullering av avtal och kan skada institutets rykte.

föreningarna att hänvisningen till föreskrifterna och allmänna råden om informationssäkerhet, it-säkerhet och insättningssystem bör tas bort då den inte uppfyller något syfte.

Finansinspektionens skäl: 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 kan riskerna reduceras. Ett företag behöver därför ha interna regler för hur detta ska göras.

Det finns olika sätt att hantera säkerhetsfrågor och Finansinspektionen lämnar till företagen att välja metod. Rent allmänt anses scenarioövningar och simuleringar vara bra metoder för att öka kunskapen kring oegentligheter som kan uppstå i ett företags verksamhet. De allmänna råden ger vägledning till företagen om lämpliga metoder. Finansinspektionen delar Bankföreningens och Fondhandlareföreningens åsikt att i det fall hot, oegentligheter och brottsliga handlingar inträffar bör detta hanteras och beslutas inom ramen för incidenthantering. Därför stryks sista meningen från de allmänna råden i remissförslaget.

En av de viktigaste tillgångarna i ett finansiellt företag är information, särskilt information om kunder och transaktioner. Mer detaljerade regler kring informationssäkerhet finns i föreskrifterna och de allmänna råden om informationssäkerhet, it-verksamhet och insättningssystem.

Med en hänvisning till föreskrifterna och allmänna om informationssäkerhet, it-verksamhet och insättningssystem tydliggörs att bestämmelserna i denna föreskrift kompletteras av bestämmelserna i 2 kap. föreskrifter om informationssäkerhet, it-verksamhet och insättningssystem.

3.4.6 Process för godkännande (5 kap. 10-14 §§)

Finansinspektionens ställningstagande: Ett företag ska ha en process för att godkänna nya, eller väsentligt förändrade produkter, tjänster, marknader, processer, it-system samt vid större förändringar i företagets verksamhet och organisation. Processen ska beskrivas i interna regler. Om det är oklart om processen ska tillämpas eller inte, ska företagets funktion för riskkontroll besluta i frågan. När företaget beslutar om en ny produkt, tjänst, process eller it-system ska det utse en person eller funktion som ska ansvara för att hantera risker förenade med dessa.

Remisspromemorian: Förslaget hade i huvudsak samma innehåll.

Remissinstanserna: *Svenska Bankföreningen* och *Svenska Fondhandlareföreningen* anser att operativa risker inte ska sammanblandas

med affärsbeslut. Analysen i processen för godkännande bör därför inte sättas i relation till företagets kapitalbehov.

Finansinspektionens skäl: Införande av nya produkter, tjänster, processer, it-system, genomförande av omorganisationer och etablering på nya marknader är naturliga och viktiga delar av affärs- och verksamhetsutvecklingen. Generellt ökar ett företags exponering för operativa risker när det exempelvis inför nya produkter eller gör större förändringar. Även om syftet med att ändra eller införa en ny produkt, process eller ett nytt it-system kan vara att minska risken i verksamheten, är själva förändringen förknippad med operativa risker. Genom att ett företag har en fastställd process för godkännande av förändringar ges möjlighet att brister och risker upptäcks i tid, vilket bör ge företaget möjlighet att agera förebyggande.

De bestämmelser om processen för godkännande som nu införs 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 nya marknader, produkter och tjänster, omfattar BCBS riktlinjer även processer och system.

I detta regelarbete har Finansinspektionen övervägt att separera processen för godkännande på de områden som omfattas av GL 44 från de områden som kommer 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. Införande av it-system som stödjer processer av väsentlig betydelse kan också medföra risker som behöver hanteras. Finansinspektionen har därför stannat vid att ha reglerna om processen som baseras på GL 44 respektive BCBS riktlinjer tillsammans. Remissinstanserna har framfört att processen för godkännande inte ska sammanblandas med affärsbeslut. Finansinspektionen anser dock att en analys av hur företagets risknivåer påverkas ska vara en integrerad del av ett affärsbeslut, och att det således är viktigt att genomföra en analys om den operativa risken påverkar kapitalbehovet. En sådan analys ska därför säkerställas inom ramen för processen för godkännande.

Finansinspektionen har i tillsynen sett att ett företag kan ha behov av att utvärdera förändringar för att kunna dra lärdom om positiva och negativa effekter av förändringen. Genom dokumentation skapas möjlighet att i efterhand utvärdera förändringen. En regel om att ett beslut om godkännande av till exempel en ny produkt ska dokumenteras införs därför. Det är också viktigt att någon på företaget har ett uttalat ansvar för förändringen. Finansinspektionen inför därför ett krav på att när ett företag beslutar om en ny produkt, tjänst, marknad, process eller it-system ska det fastställa vilken person eller funktion som ska ansvara för att hantera risker förenade med dessa.

3.4.7 Kontinuitetshantering (5 kap. 15–23 §§)

Finansinspektionens ställningstagande: Ett företag ska ha väl fungerande metoder för kontinuitetshantering. Metoderna ska omfatta beredskapsplaner, kontinuitetsplaner och återställningsplaner. För varje process som är av väsentlig betydelse ska ett företag fastställa den längst tillåtna tiden för avbrott. Ett företag ska regelbundet analysera konsekvenserna av avbrott eller större verksamhetsstörningar som kan inträffa i företagets verksamhet samt i den verksamhet som företaget har uppdragit åt någon annan. Denna analys ska genomföras på alla affärsenheter och stödfunktioner och ta hänsyn till deras beroende av varandra. Ett företag ska se till att dess huvudsakliga it-driftställe finns på ett tillräckligt stort geografiskt avstånd från den plats där företaget förvarar sina säkerhetskopior. Företaget ska ha rutiner för sin interna och externa kommunikation i samband med ett avbrott eller en större verksamhetsstörning. Ett företag ska regelbundet utbilda och informera sin personal om hur beredskapsplaner, kontinuitetsplaner och återställningsplaner används samt regelbundet uppdatera och testa planerna för att säkerställa att de är anpassade till verksamheten och prioriteringarna för att kunna återgå till normal verksamhet. Företaget ska utse ansvariga för uppdatering och test av planerna.

Remisspromemorian: Förslaget hade i huvudsak samma innehåll.

Remissinstanserna: *Svenska Bankföreningen* och *Svenska Fondhandlareföreningen* anser att begreppen beredskapsplan, kontinuitetsplan och återställningsplan bör ändras till plan för beredskap, kontinuitet och återställning, då företag använder olika namn på planerna. Föreningarna anser också att ”den längst tillåtna tiden för avbrott” ska ändras till ”acceptabla tider för avbrott”, samt att regeln om att det ska vara tillräckligt stort geografiskt avstånd mellan it-driftställe och förvar av säkerhetskopior hör bättre hemma i föreskrifterna och de allmänna råden om informationssäkerhet, it-verksamhet och insättningssystem.

Finansbolagens Förening anser att konsekvensanalyser ska genomföras årligen och inte regelbundet, samt att regeln om vilka typer av tester av beredskapsplaner, kontinuitetsplaner och återställningsplaner samt hur ofta testerna ska göras ska kunna tillämpas med proportionalitet.

Finansinspektionens skäl: I avsnitt 33 i GL 44 finns regler om kontinuitetshantering. De kontinuitetshanteringsregler som nu införs i föreskrifterna om operativa risker är främst baserade på riktlinjerna i GL 44.

Det kan finnas många orsaker till ett avbrott eller en större störning i ett företags verksamhet. Avbrott och störningar kan leda till att ett företag 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 detta så att det kan återgå till normal verksamhet inom rimlig tid. En väl fungerade kontinuitetshantering är viktig, inte bara för

företaget utan även dess kunder och det finansiella systemet som helhet. Därför införs krav på interna regler för kontinuitetshantering.

För att kontinuitetshantering ska ges det fokus och de resurser som krävs för att vara väl fungerande ska reglerna beslutas av företagets verkställande direktör. Ett företag ska också ha en skyldighet att ta fram beredskapsplaner, kontinuitetsplaner och återställningsplaner. Begreppen beredskapsplan, kontinuitetsplan och återställningsplan används i GL 44. Det saknas skäl att använda en annan terminologi i detta regelverk. Begreppen hindrar inte ett företag att namnge de interna planerna på annat sätt så länge företaget uppfyller de krav som ställs på planerna.

Finansinspektionen håller inte med Bankföreningens och Fondhandlareföreningens synpunkt att formuleringen om avbrottstider för processer av väsentlig betydelse bättre kan utryckas med ”acceptabla tider för avbrott”. Den ursprungliga formuleringen har behållits, då den enligt Finansinspektionen bättre beskriver syftet med bestämmelsen.

För att återställa en verksamhet efter ett avbrott eller en störning krävs ofta resurser, som i det skedet kan vara begränsade. Det är därför viktigt att ta fram planer i förväg. Genom att analysera de konsekvenser som ett avbrott eller en större verksamhetsstörning kan ha på verksamheten, skapas möjlighet att ta fram ändamålsenliga planer samt prioriteringar och mål inom återställningsskedet. Finansinspektionen anser inte att det är nödvändigt att ange en specifik periodicitet för genomförande av konsekvensanalysen. Det måste vara upp till varje företag att avgöra detta med hänsyn tagen till företagets specifika förutsättningar. För ett företag kan regelbundet innebära en gång per 12 månader medan det för ett annat kan vara en gång per 6 eller 18 månader.

Det geografiska avståndet mellan it-driftställe och förvaring av säkerhetskopior är en faktor för att säkerställa att ett företag har förmåga att upprätthålla verksamhet och förebygga förlust av data vid en allvarlig störning. It-driftställe och förvaringsplats för säkerhetskopior bör inte vara så nära varandra att båda ställena riskerar att slås ut av samma orsak. Även om regeln om tillräckligt geografiskt avstånd berör it-system och informationssäkerhet så anser Finansinspektionen att den i första hand avser att skapa förutsättningar för en väl fungerande kontinuitetshantering. Därför flyttas regeln inte till föreskriften om it-system, informationssäkerhet och insättningssystem.

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 beslut om huruvida beredskapsplaner, kontinuitetsplaner och återställningsplaner ska användas eller inte. Pressen på beslutsfattare ökar också i samband med större verksamhetsstörningar. Därför införs krav på rutiner för intern och extern kommunikation som en del av företagets kontinuitetshantering.

Det räcker inte med att företaget upprättar planer. För att bedöma om planerna är tillräckliga och för att öka personalens kunskap om hur dessa ska användas behöver planerna testas. En regel om test av planer införs därför.

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

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

Företag som ägnar sig åt aktiviteter på marknader för finansiella instrument och valutor är särskilt utsatta för operativa risker. Dessa verksamheter är ofta komplexa samtidigt som de omsätter höga belopp och stora volymer. Konsekvenser av operativa risker 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 även hela marknaden, eftersom förtroendet för värdepappersmarknaden kan urholkas.

Det finns i dag ingen officiell definition av vad som avses med marknadsrelaterade aktiviteter. Finansinspektionen har därför valt att avgränsa området i dessa föreskrifter till de verksamheter som faller inom ramen för de investeringstjänster och investeringsverksamheter som framgår av 2 kap. 1 § 2–3 LV och verksamheter med valutahandel som utförs med stöd av 7 kap. 1 § 12 LBF.

Reglerna i 6 kap. föreskrifterna ska därför tillämpas av de företag som har tillstånd att utföra order avseende finansiella instrument på kunders uppdrag och för handel med finansiella instrument för egen räkning enligt 2 kap. 1 § 2–3 LV samt av de företag som driver valutahandel med stöd av 7 kap. 1 § 12 LBF. Reglerna är i första hand baserade på Cebs Guidelines on the management of operational risks in market related activities.

3.5.1 Åtskillnad av arbetsuppgifter (6 kap. 2 §)

Finansinspektionens ställningstagande: Ett företag ska se till att hålla arbetsuppgifterna åtskilda mellan personal som initierar och genomför affärstransaktioner och personal som arbetar med att stödja, verifiera och övervaka dessa.

Remisspromemorian: Förslaget hade i samma innehåll.

Remissinstanserna: Hade inga synpunkter.

Finansinspektionens skäl: Genom att ha åtskillnad på arbetsuppgifter inom transaktionshanteringen och se till att den som utför eller initierar en affärstransaktion inte samtidigt kontrollerar sitt eget arbete skapas förutsättning att undvika misstag eller medveten manipulering.

3.5.2 Personal (6 kap. 3 §)

Finansinspektionens ställningstagande: Ett företag ska se till att personal som initierar och genomför affärstransaktioner, godkänner eller bekräftar affärstransaktioner, eller hanterar betalningar kopplade till affärstransaktioner, under minst tio arbetsdagar i följd under en tolvmånadersperiod, inte har möjlighet att utföra dessa arbetsuppgifter.

Remisspromemorian: Förslaget hade i huvudsak samma innehåll. I förhållande till remissförslaget har vissa redaktionella förändringar gjorts. I andra stycket i förslaget, som innebar att regeln om att även personal i funktionen för riskkontroll och de stödfunktioner som följer upp eller på något sätt hanterar transaktionen, inte har möjlighet att hantera transaktioner inte ska ha möjlighet att göra det, har tagits bort.

Remissinstanserna: *Svenska Bankföreningen* och *Svenska Fondhandlareföreningen* påpekar att bestämmelsen sammanblandar första och andra försvarslinjen och anser att den bör begränsas till att endast gälla personal som initierar och genomför affärstransaktioner, i likhet med betydelsen av termen ”traders” i Cebs vägledning.

Advokatsamfundet anser att regleringen inte anses förenlig med proportionalitetsprincipen eftersom bestämmelsen exempelvis träffar ett värdepappersbolag med ett fåtal anställda som har tillstånd att ta emot och vidarebefordra order. Man menar att det inte finns några tungt vägande argument för att tanken att reglering av denna art behöver införas för små värdepappersbolag med begränsad verksamhet.

Finansinspektionens skäl: Betydande förluster har uppstått i värdepappers- och valutahandelsrörelser till följd av att personer med god insikt i hur företagets kontrollsystem fungerar (till exempel handlare med ett förflutet inom en stödfunktion) under en längre tid har kunnat dölja växande förluster i felaffärer eller bedrägerier. Exempel på sådant agerande är att positioner har dolts genom att ha flyttats runt mellan olika konton eller medvetet har värderats fel. Om personal med vissa arbetsuppgifter inte har möjlighet att utföra dessa under en sammanlagd tidsperiod på åtminstone 10 arbetsdagar per år blir det lättare för ett företag att upptäcka denna typ av manipulationer. En sådan bestämmelse ska inte begränsas till att enbart avse de som initierar och genomför affärstransaktioner utan även de som godkänner och bekräftar sådana transaktioner, liksom personal som hanterar betalningar till sådana transaktioner. Regeln hindrar inte att ett företag beslutar att låta även andra befattningshavare omfattas av detta förfaringssätt.

Uppskattningsvis kommer regeln omfatta ca 90 värdepappersföretag samt de företag som bedriver valutahandel. Dessa företag har en typ av reglerad verksamhet som ska kunna skötas löpande och måste därför vid var tid kunna hantera personalsituationen utan att verksamheten stannar upp vid semestrar, ledighet, sjukdom och dylikt. Finansinspektionen bedömer att det saknas skäl att införa proportionalitet för bestämmelsen.

Advokatsamfundets synpunkt har beaktats i och med att tillämpningsområdet för 6 kap. har begränsats i förhållande till remissförslaget.

3.5.3 Transaktionshantering (6 kap. 4 §)

Finansinspektionens ställningstagande: För att kunna ha kontroll över de operativa riskerna ska varje transaktion vara dokumenterad och spårbar till handlaren. Det ska finnas rutiner och kontroller från öppnandet av en affärsrelation till avveckling av utförda transaktioner. Villkor för transaktionen ska dokumenteras och bekräftas innan handel påbörjas. Tiden från initierande av en transaktion till dess att stödfunktioner kan stämma av, bekräfta, avveckla och följa upp transaktionen ska vara kort. Det ska finnas rutiner för att hantera och rapportera felaktigt utförda transaktioner och obekräftade affärer. Transaktioner, likvider och positioner ska dagligen stämmas av.

Remisspromemorian: Förslaget hade i huvudsak samma innehåll. I förhållande till remissförslaget har dock vissa förtydliganden och justeringar gjorts med anledning av remissinstansernas synpunkter.

Remissinstanserna: *Svenska Bankföreningen* och *Svenska Fondhandlareföreningen* anser att information avseende transaktioner som har gett upphov till missförstånd som företaget och motparten inte kan lösa omgående, ska rapporteras till stödfunktionerna. Först därefter sker, om förutsättningar föreligger enligt de interna riktlinjerna, rapportering till andra linjens riskkontroll.

Finansinspektionens skäl: För att ett företag ska kunna upptäcka, utreda och analysera olika typer av fel eller avvikelser införs regler kring verifieringskedjan för varje transaktion.

Villkor för transaktionen ska dokumenteras och bekräftas innan handel påbörjas. Dokumentation och bekräftelse bör kunna göras så väl skriftligt som genom ljudupptagning. I praktiken innebär detta att de normala villkoren kan dokumenteras och bekräftas vid den initiala affärskontakten medan alla transaktioner med villkor som avviker från de normala dokumenteras och bekräftas inför varje transaktion. Genom dokumenterade och bekräftade villkor bör risken minska för att till exempel affärer måste makuleras därför att avveckling inte kan ske.

För att undvika osäkerhet och minimera negativa ekonomiska konsekvenser samt minska risken för oegentligheter, ska ett företag sträva efter att så långt

som möjligt inte ha affärer som är obekräftade. Detta för att säkerställa att det inte råder oenighet om vilken part som står för risken. Därför är det lämpligt att personal som initierar och genomför affärstransaktioner så snart som möjligt efter ett affärsavslut lämnar nödvändig information och dokumentation till stödfunktionerna så att de så snart som möjligt kan stämma av, bekräfta, avveckla och följa upp transaktionen.

Ett företag ska ha fastställda rutiner för hantering och rapportering av felaktigt utförda transaktioner. Rutinerna bör bland annat ange de åtgärder som ska vidtas för att utreda vad som har avtalats, vem som vidtar åtgärderna, vem som bedömer risken i ”felaffären” samt vem som fattar beslut om vad som ska göras om affären till exempel behöver stängas och vilka personer i företaget som ska informeras.

Om obekräftade affärer kvarstår, 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.

Slutligen införs ett krav på daglig avstämning av transaktioner, likvider och positioner. Det finns en risk att positioner medvetet eller omedvetet registreras på konton som inte är aktiva och inte är spärrade för registrering. Därför är det viktigt att även sådana konton, liksom alla interna konton, blir föremål för daglig avstämning.

3.5.4 Hantering av säkerheter (6 kap. 5–6 §§)

Finansinspektionens ställningstagande: Ett företag ska ha rutiner för att hantera och kontrollera säkerheterna i samband med transaktioner och positioner och se till att det finns fastställda rutiner för kontroll av utrymme inom motpartslimiter innan dessa utnyttjas vid handel.

Remisspromemorian: Förslaget hade i huvudsak samma innehåll.

Remissinstanserna: *Svenska Bankföreningen* och *Svenska Fondhandlareföreningen* anser att paragrafen om att ett företag ska ha it-system som under pågående handel löpande kan sammanställa information om hur företaget utnyttjar motpartslimiter bör strykas. Oavsett var en sådan funktionalitet placeras så bedömer föreningarna inte att detta begränsar riskerna. Föreningarna anser att kostnadsaspekten behöver analyseras mer utförligt med hänsyn till den administrativa börda ett sådant krav skulle innebära för att få ett it-system på plats.

Finansinspektionens skäl: Genom att företag har metoder för att vid var tid ha kontroll på motspartlimiter minskas riskerna för att limiter överträds, till exempel på grund av misstag eller vid värdeförändring i underliggande

säkerhet. Det optimala torde vara att företag har realtidssystem för denna kontroll, men som remissinstanserna framfört kan den administrativa bördan att införa sådana system bli betydande. Eftersom Finansinspektionen anser att det är viktigt att det utförs kontroll av utrymme inom motpartslimiter innan dessa utnyttjas vid handel införs krav på kontrollrutiner. Finansinspektionen överlämnar till det enskilda företaget att avgöra på vilket sätt detta krav ska uppnås.

3.5.5 Övervakning och kontroll (6 kap. 7–11 §§)

Finansinspektionens ställningstagande: Ett företag ska vid väsentliga avvikelser eller orimliga resultat relaterat till handel analysera om dessa är orsakade av misstag, oegentligheter eller andra händelser i verksamheten. Företaget ska löpande granska och stämma av sina konton. Ett företag ska kontrollera värdet på sina nettopositioner och de transaktioner som ger upphov till dessa, samt fastställa och regelbundet följa upp limiter för sina positioner. Limiterna ska sättas på ett sätt som gör det är möjligt att följa upp och kontrollera dem. Minst en gång i kvartalet ska företaget kontrollera att behörigheter till de it-system som används i verksamheten är begränsade till behov utifrån tilldelade arbetsuppgifter.

Remisspromemorian: Förslaget hade samma innehåll.

Remissinstanserna: *Svenska Bankföreningen* och *Svenska Fondhandlareföreningen* anser inte att det är rimligt att behörighetskontroller ska ske varje kvartal utan att frekvensen bör anpassas till den verksamhet som kontrolleras. De anser att det är mer lämpligt att uppställa ett krav om kontroll minst två gånger per år.

Finansinspektionens skäl: 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.

Resultatanalys är ett viktigt komplement till andra analyser och kontroller. Ett resultat som avviker från det normala kan vara en indikation på att något har blivit fel, medvetet eller omedvetet. Genom att kritiskt granska resultatet kan manipulation som inte har fångas upp genom andra kontroller hittas. Därför har föreskrivits att väsentliga avvikelser och orimliga resultat vid värdepappers- och valutahandel ska analyseras för att bedöma att de är marknadsrelaterade och utesluta att de beror på misstag, medveten manipulation, andra oegentligheter eller andra händelser hänförliga till operativa risker. 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.

Liksom vid den dagliga avstämningen är det viktigt att såväl samtliga aktiva som inaktiva konton kontrolleras. Därför införs en specifik bestämmelse om att företagets konton löpande ska granskas och stämmas av. Syftet med bestämmelsen är 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 olika 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 införs regeln att kontroller av värdet på nettopositioner kompletteras med kontroll av de transaktioner som ger upphov till dessa. Tanken är att göra en djupare analys av riskbilden i positionen och att fånga upp misstag, felbedömningar eller medveten manipulering av positionen.

Finansinspektionen inför en regel att ett företag ska fastställa och regelbundet följa upp limiter för sina positioner. Limiterna ska sättas på en sådan detaljerad nivå att uppföljning och kontroll kan göras. På det sättet kan företaget, förutom att kontrollera att uppsatta limiter följs, spåra vem som brutit mot limiten eller vad som är orsaken till överträdelsen.

Finansinspektionen inför en bestämmelse om att ett företag minst kvartalsvis ska kontrollera behörigheter till it-system inom värdepappersrörelsen och valutahandeln. Bestämmelsen är således strängare än bestämmelsen i 3 kap. 8 § föreskrifterna och de allmänna råden om informationssäkerhet, it-verksamhet och insättningssystem, som ställer krav på minst en årlig kontroll. Bestämmelsen om kvartalsvisa kontroller har sin bakgrund i att dessa verksamheter är extra utsatta för operativa risker. Hanteringen av behörigheter, så att dessa alltid är aktuella och uppdaterade med hänsyn till personalens aktuella tjänster och arbetsuppgifter, är därför en viktig åtgärd för att hantera riskerna. Mindre frekventa kontroller bedöms inte vara tillräckliga. Finansinspektionen har vid sin tillsyn inte sällan konstaterat brister i hanteringen av behörigheter.

4 Nya regler om informationssäkerhet, it-verksamhet, och insättningssystem

Remissförslaget hade en annan struktur med kapitelrubrikerna it-system, informationssäkerhet och insättningssystem. Efter påpekande från Svenska Bankföreningen om att innehållet i kapitlet om it-system tydligare återspeglas med begreppet it-verksamhet har Finansinspektionen ändrat rubriken på kapitlet. Dessutom har kapitlet om informationssäkerhet och it-verksamhet bytt plats. Med dessa ändringar justeras föreskriftens namn och de avser inte någon ändring i sak.

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

Reglerna i kapitel 2 och 3 kompletterar föreskrifterna om hantering operativa risker avseende krav av informationssäkerhet och it-verksamhet. Det fjärde 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 i samma ordning som kapitlen i föreskrifterna. I vissa fall kommenteras enskilda paragrafer och begrepp.

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

- informationssäkerhet,
- it-verksamhet, och
- insättningssystem.

4.1 Informationssäkerhet (2 kap.)

Informationssäkerhet syftar till att skydda information. Med att skydda information avser Finansinspektionen att kunna upprätthålla rätt nivå av konfidentialitet, riktighet och tillgänglighet på informationen.

Att åstadkomma och upprätthålla tillräcklig informationssäkerhet 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.

4.1.1 Ledningssystem för informationssäkerhet (2 kap. 1 §)

Finansinspektionens ställningstagande: Ett företag ska arbeta strukturerat och metodiskt med informationssäkerhet genom att använda sig av ett ledningssystem.

Remisspromemorian: Remissförslaget innehöll väsentligen samma förslag men även en sammanfattning av 2–9 §§.

Remissinstanserna: Remissinstanserna hade inga synpunkter.

Finansinspektionens skäl: Ett strukturerat och metodiskt arbete med informationssäkerhet är en förutsättning för att skapa och upprätthålla informationssäkerhet. Information, särskilt om kunder och transaktioner, är en av ett företags viktigaste tillgångar. Finansinspektionen anser därför 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 utformandet av bestämmelserna i detta kapitel. Detta innebär dock inte att Finansinspektionen ställer krav på att ett företag ska certifiera sig mot denna standard. Finansinspektionen är emellertid positiv till användningen av standarder som stöd i ett företags arbete med informationssäkerhet. Standarder bygger vanligtvis på redan gjorda erfarenheter och gör det därigenom möjligt för användaren av en standard att ta tillvara redan gjorda landvinningar. På så sätt kan det vara lättare att uppnå rätt säkerhet och undvika onödiga misstag.

Tillämpning av allmänt etablerade standarder såsom SS-ISO/IEC 27001 och svensk standard ”riktlinjer för styrning av informationssäkerhet” SS-ISO/IEC 27002 kan även bidra till att öka transparensen mellan företag såväl som mot leverantörer av exempelvis it-tjänster. Det kan göra det lättare att ställa krav och bedöma produkter, system och hela verksamheter.

4.1.2 Mål och inriktning (2 kap. 2 §)

Finansinspektionens ställningstagande: Ett företag ska fastställa och dokumentera mål och inriktning med sitt informationssäkerhetsarbete. Styrelsen eller den verkställande direktören ska besluta om målen och inriktningen på informationssäkerhetsarbetet.

Remisspromemorian: Remissförslaget innehöll väsentligen samma förslag.

Remissinstanserna: *Svenska Bankföreningen* föreslår att begreppet ”informationssäkerhetsarbete” ersätts med ”informationssäkerhet”. *Riksgälden* föreslår även att ett krav läggs till om att ett företags ledning löpande informerar sig om arbetet med informationssäkerhet samt minst en gång per år följer upp och utvärderar informationssäkerhetsarbetet.

Finansinspektionens skäl: För att informationssäkerhetsarbetet ska ges det fokus och de resurser som krävs måste ett företags mål och inriktning med informationssäkerhetsarbetet beslutas av företagets verkställande direktör eller styrelse.

Begreppet ”informationssäkerhetsarbete” ändras till ”informationssäkerhet” i enlighet med Bankföreningens förslag. Syftet med bestämmelsen är att företagets styrelse eller verkställande direktör ska besluta om övergripande mål och inriktning med informationssäkerheten. Genom ändringen blir det tydligare att det inte handlar om detaljer i informationssäkerhetsarbetet.

Genom föreskrifterna om styrning, riskhantering och kontroll ställs krav om rapportering om företagets risker till styrelse och den verkställande direktören. Föreskrifterna om hantering av operativa risker ställer även särskilt krav på rapportering av operativa risker till styrelsen. Mot bakgrund av att Finansinspektionen anser att ett företags informationssäkerhet och arbete med informationssäkerhet är en del av dess hantering av operativa risker anser Finansinspektionen inte att det i dagsläget är motiverat att specificera närmare krav avseende ledningens uppföljning och utvärdering av informationssäkerheten.

4.1.3 Ansvar och samordning (2 kap. 3–4 §§)

Finansinspektionens ställningstagande: Ett företag ska säkerställa att det är tydligt hur ansvaret för informationssäkerheten inom verksamheten är fördelad. Ett företag ska utse en person som ansvarar för att leda och samordna arbetet med informationssäkerhet.

Remisspromemorian: Förslaget hade samma innehåll.

Remissinstanserna: *Svenska Bankföreningen* föreslår att kraven i 3 och 4 §§ slås samman och kondenseras som ”ett företag ska säkerställa att det är tydligt hur ansvaret för informationssäkerheten leds, samordnas och fördelas”. Vidare för Bankföreningen fram att informationssäkerheten i en bankkoncern med flera legala affärsenheter och etableringar i flera länder leds av flera personer. Om bestämmelsen ska kvarstå anser Bankföreningen att en funktion och inte en person ska utses. *Finansbolagens Förening* anser att uppgiften att leda och samordna informationssäkerhetsarbetet av proportionalitetsskäl även kunna utföras av en relevant funktion.

Finansinspektionens skäl: Kravet om att företaget ska utse en person syftar dels till att informationssäkerhetsarbetet ska ges tillräckligt fokus, dels till att det ska vara tydligt vem det är som har det övergripande ansvaret för att leda och samordna företagets arbete med informationssäkerhet. Finansinspektionen bedömer att det även i bankkoncerner med flera legala affärsenheter samt med verksamhet i flera länder bör vara möjligt att utse en person med det övergripande ansvaret för att leda och samordna arbetet med informationssäkerhet, vilket är förekommande i koncerner inom områden som exempelvis ekonomi, riskkontroll och it.

4.1.4 Informationsklassificering och riskanalys (2 kap. 5–6 §§)

Finansinspektionens ställningstagande: Ett företag ska klassificera sin information för att den ska få rätt skyddsnivå. Klassificeringen ska utgå från de krav som ställs på informationens konfidentialitet, riktighet och tillgänglighet i verksamheten. Företaget ska dokumentera denna klassificering och utse personer eller funktion som ansvarar för den information som hanteras inom

verksamheten. Företaget ska även analysera risker hänförliga till företagets informationssäkerhet och besluta om hur det ska hantera dessa.

Remisspromemorian: Förslaget hade i huvudsak samma innehåll.

Remissinstanserna: S*venska Bankföreningen* föreslår att ”organisatorisk enhet” i 2 kap. 5 § ändras till ”funktion”.

Finansinspektionens skäl: Finansinspektionen ändrar 2 kap. 5 § i enlighet med Bankföreningens förslag. Då begreppet funktion, som finns definierad i föreskrifterna om styrning, riskhantering och kontroll är organisatoriska enheter, innebär ändringen inte någon förändring i sak.

Informationssäkerhet definieras i föreskrifterna som skydd av konfidentialitet, riktighet och tillgänglighet hos information. Finansinspektionen har även definierat konfidentialitet, riktighet och tillgänglighet och i detta arbete utgått från SIS Handbok 550 (version 3).

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 relaterade risker kan ett företag fatta relevanta beslut om lämpliga skyddsåtgärder för informationen i verksamheten.

Finansinspektionen anser vidare att det är viktigt av spårbarhetsskäl att klassificeringen dokumenteras.

4.1.5 Interna regler (2 kap. 7–9 §§)

Finansinspektionens ställningstagande: Ett företag ska fastställa interna regler för sitt arbete med informationssäkerhet. Reglerna bör ange krav på fysisk säkerhet, skydd av datakommunikation och drift, spårbarhet i it-system, att produktionsmiljön för it-system är separerad från test- och utvecklingsmiljöer, styrning av åtkomst till information, säkerhetskrav på it-system vid inköp, utveckling, underhåll och avveckling, rapportering och hantering av informationssäkerhetsrelaterade incidenter, och regelbunden kontroll av företagets it-system mot den fastställda skyddsnivån för information. Åtkomstbehörigheter ska kontrolleras minst årligen.

Remisspromemorian: Förslaget hade i huvudsak samma innehåll.

Remissinstanserna: *Svenska Bankföreningen* anser att de allmänna råden bör flyttas till remisspromemorian och att syftet skulle bli tydligare om punkt 2

delades upp i tre punkter. Vidare föreslår Bankföreningen att begreppet ”produktionsmiljö” används istället för ”driftsmiljö”. *Datainspektionen* anser att de allmänna råden i punkt 4 bör inkludera avveckling till följd av risken för att bland annat personuppgifter kan läcka ut till obehöriga i samband med avvecklingen. Av samma skäl anser Datainspektionen att de allmänna råden i punkt 1 i förslagets 3 kap. 4 § om processer bör inkludera avveckling.

Finansinspektionens skäl: Finansinspektionen ändrar föreskrifterna enligt remissinstansernas förslag.

Bestämmelsen i 2 kap. 7 § innehåller en proportionalitetsprincip som innebär att företagen ska beakta arten, omfattningen och komplexiteten i sin verksamhet när det utformar de interna reglerna för informationssäkerhet. Genom proportionalitetsprincipen tydliggörs att olika företags interna regler för informationssäkerhet kan ha, och i realiteten ofta har, olika omfattning och utformning.

Till kravet på att det ska finnas fastställda interna regler lämnar 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 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 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. För kritisk funktionalitet är det lämpligt att sträva efter att minimera beroendet av enskilda komponenter.

Spårbarhet i it-system
Finansinspektionen anser i sammanhanget att det är viktigt att ett företag fastställer krav på vilka aktiviteter i it-systemen som är av betydelse för informationssäkerheten och som därför ska vara spårbara. Finansinspektionen har definierat begreppet spårbarbarhet och i detta arbete utgått från SIS Handbok 550 (version 3). Spårbarhet gör det möjligt att i efterhand härleda ursprung och/eller förändringar av en aktivitet. 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. Spårbarheten bör normalt vara så detaljerad att den kan användas för att utreda felaktig eller obehörig användning av information.

Separation av produktionsmiljö från test- och utvecklingsmiljöer
För att förhindra obehörig åtkomst till eller ändringar i företagets produktionsmiljö, samt driftsavbrott bör ett företag även fastställa den nivå på separation mellan produktionsmiljö respektive test- och utvecklingsmiljöer som är nödvändig för att säkerställa en säker drift av företagets it-system.

Styrning av åtkomst till information
Åtkomst till information och it-system bör styras utifrån verksamhets- och säkerhetskrav.

De interna reglerna om styrning av åtkomst ska särskilt inkludera krav på åtkomstbehörigheter till it-system enligt 3 kap. 8 §.

Vid utformandet av interna regler på området kan det exempelvis vara aktuellt att beakta krav på loggning och uppföljning, detta vid informationsbehandling såväl inom företaget som vid samverkan med andra företag. Vidare kan det vara relevant att beakta krav på användningen av höga behörigheter. Detta särskilt då denna typ av behörigheter, även kallade administrativa/priviligierade behörigheter, gör det möjligt att förbigå system- eller tillämpningskontroller till it- system vilket kan medföra väsentliga risker för fel eller intrång. Ytterligare exempel är lösenordshantering, styrning av åtkomst till nätverk samt mobil datoranvändning och distansarbete.

Säkerhetskrav på it-system vid inköp, utveckling, underhåll och avveckling
För att säkerställa att informationssäkerheten integreras i företagets it-system är det viktigt att ett företag tar hänsyn till verksamhetens säkerhetskrav under systemens livscykel. Inköp, utveckling och underhåll kan ses som faser i ett systems livscykel där avveckling kan ses som en avslutande fas. Av kraven i 2 kap. 5 § följer att ett företag ska klassificera informationen utifrån bland annat krav på konfidentialitet. Informationen finns ofta i it-systemen, till exempel på hårddiskar. Datainspektionens förslag att lägga till ”avveckling” i de allmänna rådens punkt 6 kan således ses som tydliggörande av vad som gäller för konfidentialitet för information i ett avvecklingsskede av it-systemen. Då innebörden av tillägget får anses följa redan av existerande krav i föreskrifterna och förändringen inte bedöms som betungande för ett företag anses tillägget inte vara av sådan art eller omfattning att förändringen har behövt remitteras särskilt (se 4.2.4).

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. Därmed uppnås koppling till bestämmelsen i 3 kap. 6 § föreskrifterna om hantering av operativa risker.

Regelbunden kontroll av den fastställda skyddsnivån
De allmänna råden om regelbunden kontroll syftar till att säkerställa att den klassificerade skyddsnivån återspeglas i praktiken. Finansinspektionen anser att principerna för företagets kontroll bör fastställas i företagets interna regler.

4.2 It-verksamhet (3 kap.)

I definitionen av operativ risk ingår bland annat system. Reglerna i kapitlet tar, genom kopplingen till hanteringen av företagens it-system, sikte på it-verksamheten hos ett företag. 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 samt att det ska finnas ändamålsenliga processer och rutiner för hanteringen av systemen.

4.2.1 Säkerhet (3 kap. 1 §)

Finansinspektionens ställningstagande: Ett företag ska se till att dess it-system är tillräckligt säkra i förhållande till arten hos den information som företaget hanterar i systemen.

Remisspromemorian: Förslaget hade samma innehåll.

Remissinstanserna: *Svenska Bankföreningen* anser att det bör stå fritt för företagen att använda sin riskhanteringsmodell i linje med föreskriften för operativ risk och föreslår att de allmänna råden, om att utgå från informationsklassificeringen vid bedömning om it-systemen är tillräckligt säkra, flyttas till remisspromemorian.

Finansinspektionens skäl: Det har tidigare i denna promemoria framhållits att finansiella företag är 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.

De grundläggande reglerna om att ett företag ska ha ändamålsenliga it-system och rutiner för att skydda konfidentialitet, riktighet och tillgänglighet i dess information finns för kreditinstitut och värdepappersbolag i 2 kap. 2 § föreskrifterna om styrning, riskhantering och kontroll samt i 6 kap. 2 § värdepappersföreskrifterna.

Ett finansiellt företag har vanligtvis många olika it-system som stöd 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 grad av konfidentialitet som gäller informationen som hanteras i systemen. Vad som är tillräckligt säkert måste därför bedömas från fall till fall.

En lämplig utgångspunkt är dock att koppla denna bedömning till den information som it-systemet hanterar. I förslagets andra kapitel ställer Finansinspektionen krav på att ett företag ska klassificera sin information utifrån krav på konfidentialitet, riktighet och tillgänglighet. När det gäller bedömningen om it-systemen är tillräckligt säkra ger Finansinspektionen därför ett allmänt råd med innebörden att företagen bör utgå från klassificeringen av informationen när det bedömer kraven på it-systemen.

Finansinspektionen delar inte Bankföreningens synpunkt om att de allmänna råden bör flyttas till remisspromemorian, utan anser att de allmänna råden är av betydelse för att ge vägledning om hur kraven på it-system i föreskrifterna om styrning, riskhantering och kontroll och värdepappersföreskrifterna bör läsas i förhållande till kraven på informationsklassificering i 3 kap. i denna föreskrift.

4.2.2 Mål och strategi (3 kap. 2 §)

Finansinspektionens ställningstagande: Ett företag ska ha dokumenterade övergripande mål och strategier för sin it-verksamhet. Den verkställande direktören ska besluta om företagets övergripande mål och strategier för it-verksamheten, och regelbundet utvärdera och uppdatera dessa om det behövs.

Remisspromemorian: Förslaget hade i huvudsak samma innehåll.

Remissinstanserna: *FAR* anser att ett företags it-strategi ska fastställas av företagets styrelse. Detta då it-verksamheten är central för finansiella företag och att val av it-strategi är av mycket stor betydelse för ett finansiellt företags fortsatta framgång och effektivitet.

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

It-verksamhet utgör en 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 ges enligt Finansinspektionen tillräckliga förutsättningar för att it-verksamheten får den

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

Finansinspektionens utgångspunkt är att den betydelse som it-verksamheten har för finansiella företag medför att de aspekter som Advokatsamfundet tar upp i sitt yttrande redan i dag vanligtvis beaktas i de övergripande strategier som en styrelse i ett finansiellt företag redan har att fastställa.

4.2.3 Ansvariga (3 kap. 3 §)

Finansinspektionens ställningstagande: Ett företag ska säkerställa att det är tydligt vem som ansvarar för de olika delarna av företagets it-verksamhet. För varje it-system ska företaget utse en person eller funktion som ansvarar för företagets krav på systemet.

Remisspromemorian: Remissförslaget innehöll väsentligen samma förslag.

Remissinstanserna: *Svenska Bankföreningen* föreslår att ordet ”it-organisation” ersätts med ”it-verksamhet”, att ordet ”systemägare” tas bort då det inte används av alla banker och att begreppet ”organisatorisk enhet” ersätts med ”funktion”.

Finansinspektionens skäl: I förhållande till remissförslaget ändras bestämmelsen så att ordet ”it-organisation” ersätts med ”it-verksamhet” för att skapa en ökad enhetlighet genom kapitlet genom användning av begreppet ”it-verksamhet”. Organisatorisk enhet ersätts med funktion, se 3.4.1. Ordet ”systemägare” tas bort. I stället beskrivs den roll som den ansvarige har att definiera och kommunicera krav avseende bland annat funktionalitet och säkerhet på ett it-system. I praktiken innebär det för ett flertal system att det främst är affärsverksamhetens krav. Ändringarna avser inte medföra några förändringar i sak.

4.2.4 Processer (3 kap. 4 §)

Finansinspektionens ställningstagande: Ett företag ska ha ändamålsenliga processer för hur det hanterar sina it-system. Företaget ska dokumentera processerna och beskriva de förhållanden som är av betydelse för att kunna hantera dess it-system på ett kontrollerat sätt. Sådana processer som bör vara dokumenterade omfattar inköp, utveckling, underhåll, avveckling, drift, incidenthantering, ändringshantering och test.

Remisspromemorian: Förslaget hade i huvudsak samma innehåll. Process för avveckling av it-system saknades dock i förslaget.

Remissinstanserna: *Svenska Bankföreningen* föreslår att identitets- och behörighetshantering läggs till i listan över processer i de allmänna råden. *Finansbolagens Förening* anser att ett väsentlighetskriterium behöver kopplas

till kravet om vilka förhållanden som ett företag ska dokumentera avseende processerna och de förhållanden som är av väsentlig betydelse bör begränsas.

Datainspektionen instämmer i Finansinspektionen förslag till allmänna råd om vilka processer ett företag bör dokumentera. Datainspektionen anser vidare att det är viktigt att ett företag har ändamålsenliga processer även i samband med avveckling av it-system då undermåliga processer på detta område kan medföra risk för att bland annat personuppgifter läcker ut till obehöriga i samband med avvecklingen.

Finansinspektionens skäl: 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. Därför införs 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 allmänna råd anger Finansinspektionen ett antal processer som bör finnas dokumenterade. Processerna i de allmänna råden ska inte ses som en uttömmande lista.

Finansinspektionen beaktar Datainspektionens förslag och lägger till ”avveckling” i listan över processer i de allmänna råden över vilka processer som bör finnas dokumenterade, se avsnitt 4.1.5.

Finansinspektionen har övervägt Bankföreningens krav om att inkludera identitets- och behörighetshantering i listan över processer i de allmänna råden men anser att de allmänna råden om interna regler för informationssäkerhet i 3 kap. 7 § och kraven i 3 kap. 8 § är tillräckliga.

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

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

Inköp, utveckling och förvaltning och avveckling
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 som ska 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. Bristande rutiner vid avveckling av it-system och utrustning med lagringsmedia kan medföra att konfidentiell information läcker ut till obehöriga. Det är därför viktigt att ett företag även har en ändamålsenlig process för avveckling av it-system.

Drift
Driften av ett it-system är förknippad med dagliga och regelbundna aktiviteter. Brister i dessa kan få stora konsekvenser på riktigheten och tillgängligheten hos det data som systemen hanterar. Ett företag bör därför ha dokumenterade processer och rutiner för sin drift. Med dokumenterade processer för drift avses att de åtgärder och funktioner som behövs för den dagliga driften av företagets it-system är formaliserade och att arbetet med driften i så stor utsträckning som möjligt ska kunna följas upp i efterhand.

Incidenthantering
Incidenter som i varierande grad 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, bör ett företag 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 dessa, samt att 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. Ett företag bör därför ha en process för att hantera ändringar som kan påverka företagets it-system och informationshantering.

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

4.2.5 Dokumentation över it-system (3 kap. 5 §)

Finansinspektionens ställningstagande: Ett företag ska ha en dokumentation över varje enskilt it-system som är av betydelse för verksamheten. Vilka

systemen är ska framgå av en förteckning som regelbundet ska ses över och uppdateras om det behövs.

Remisspromemorian: Förslaget hade i huvudsak samma innehåll

Remissinstanserna: *Finansbolagens Förening* anser att endast it-system av väsentlig betydelse ska behöva leva upp till kravet om att det ska finnas en dokumentation.

Finansinspektionens skäl: Finansinspektionen ersätter ”uppdateras regelbundet” med ”utvärderas regelbundet och utvärderas om det behövs” för att anpassa skrivningen till liknande skrivningar i föreskrifterna. Eftersom företagen blir allt mer beroende av it-system för att hantera sin information och systemen samtidigt blir allt mer sammanlänkande håller Finansinspektionen inte med Finansbolagens Förening om att endast it-system av väsentlig betydelse ska behöva leva upp till dokumentationskravet.

Genom att it-systemen dokumenteras och att det tydliggörs hur de fungerar och vilka beroenden systemen har minskar även personberoenden i verksamheten och en intern kunskapsbank säkerställs. Exempel på aspekter som kan beaktas i dokumentationen är beskrivning av hur systemet är avsett att användas, hur systemet fungerar och ska underhållas samt vad som krävs för den dagliga driften av systemet.

4.3 Insättningssystem (4 kap.)

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.[17]

Reglerna i detta kapitel följer den struktur som presenteras i regeringens proposition 2010/11:109 om ändringar i insättningsgarantin gällande

[17] 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.

utformningen av krav på it-system för hantering av information om insättare och deras insättningar.[18]

4.3.1 Riskanalys (4 kap. 3 §)

Finansinspektionens ställningstagande: Ett företag ska årligen analysera de risker som är hänförliga till de it-system som företaget använder för att hantera information om insättare och deras insättningar. Analysen ska innefatta skyddet för informationens riktighet och systemintegriteten hos it-systemet. Analysen ska även omfatta informationens konfidentialitet och tillgänglighet. Med systemintegritet avses i detta kapitel att ett it-system kan upprätthålla sin avsedda funktion och därigenom skyddas mot oönskad påverkan, ändring eller insyn.

Remisspromemorian: Förslaget hade i huvudsak samma innehåll.

Remissinstanserna: *Svenska Bankföreningen* anser att definitionen av systemintegritet ska flyttas till stycket med definitioner i 1 kap. alternativt att det förtydligas att definitionen avser aktuellt kapitel och inte föreskrifterna som helhet.

Finansinspektionens skäl: I förhållande till remissförslaget ändras definitionen av ”systemintegritet” genom att ”i dessa föreskrifter” ersätts med ”i detta kapitel”. Ändringen innebär ingen ändring i sak.

4.3.2 Funktioner och rutiner (4 kap. 4 §)

Finansinspektionens ställningstagande: Ett företag ska se till att det finns tekniska funktioner och administrativa rutiner för att säkerställa åtkomstkontroll, att aktiviteter i it-system och ändringar av it-system är spårbara, systemintegritet och informationens riktighet. Vidare ska systemets drift kunna återställas efter avbrott och informationen om insättare och insättningar vara tillgängliga i enlighet med Riksgäldens föreskrifter (RGKFS 2011:2) om instituts skyldighet att lämna uppgifter om insättare och deras insättningar även i samband med avbrott.

Företaget ska dessutom besluta vilka ytterligare tekniska funktioner och administrativa rutiner som är nödvändiga utifrån de riskanalyser det ska utföra enligt 3 §.

Remisspromemorian: Jämfört med förslaget ändras kravet i punkt 5 genom att kravet på att återställa systemet ”utan dröjsmål” tas bort. En punkt 6 läggs till som tar sikte på informationens tillgänglighet.

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

Remissinstanserna: *Svenska Bankföreningen* anser att begreppet ”utan dröjsmål” i punkt 5 i förslaget behöver definieras i remisspromemorian och att det skulle vara för långtgående att med utgångspunkt från kraven i 6 kap. 3a § § LBF ålägga företag att alltid utan dröjsmål kunna återställa systemets drift inom ett dygn oavsett vari grunden till problemet ligger. Föreningen menar att ett företag utifrån LBF alltid måstet kunna uppfylla kravet i LBF på ett eller annat sätt oaktat när i tiden systemets drift kan återställas. *Finansbolagens Förening* anser att kravet om ”utan dröjsmål” i punkt 5 behöver förtydligas alternativt utgå.

Finansinspektionens skäl: 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 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 tekniska funktioner för att säkerställa systemets integritet.

Med utgångspunkt från Bankföreningens och Finansbolagens Förenings synpunkter ersätts tidskriteriet för systemet återställning i 4 kap. 4 § p 5 med en kompletterande sjätte punkt som tar sikte på tillgängligheten hos den information som systemet hanterar och kopplar detta till kraven i Riksgäldens föreskrifter (RKGFS 2011:2) om instituts skyldighet att lämna uppgifter om insättare och deras insättningar.

4.3.3 Dokumentation (4 kap. 5 §)

Finansinspektionens ställningstagande: Ett företag ska utöver de krav som anges i 3 kap. 5 § dokumentera de tekniska funktioner och administrativa rutiner som ett företag ska ha enligt 4 §. Dokumentationen ska regelbundet ses över och uppdateras om det behövs.

Remisspromemorian: Förslaget hade i huvudsak samma innehåll. Kraven på att dokumentationen ska uppdateras regelbundet ersätts dock med regelbundet ses över och uppdateras vid behov.

Remissinstanserna: *Svenska Bankföreningen* föreslår att ordet ”särskilt” stryks ur första meningen och att andra meningen ändras till att ”dokumentationen ska uppdateras vid behov” för att säkerställa att dokumentationen är vid var tid aktuell. *Finansbolagens Förening* förespråkar att kravet, om att dokumentation uppdateras ”regelbundet” ändras till ”vid

behov”. Om skrivning behålls anser föreningen även att periodiciteten bör anges och att årligen är en rimlig periodicitet.

Finansinspektionens skäl: Ordet ”särskilt” utelämnas i enlighet med Bankföreningens förslag för att öka tydligheten i bestämmelsen. De övriga ändringarna syftar till att anpassa formuleringarna till övriga delar av föreskrifterna och bedöms inte ha någon påverkan i sak.

4.3.4 Granskning och rapportering (4 kap. 6 §)

Finansinspektionens ställningstagande: Företagets funktion för internrevision ska årligen granska företagets insättningssystem samt de tekniska funktioner och administrativa rutiner som är av betydelse för säkerheten i systemet. Om företaget saknar en funktion för internrevision ska det uppdra den årliga granskningen till någon som har särskild kompetens inom säkerhetsområdet. Granskningen ska dokumenteras och rapporteras till företagets styrelse. Granskningen bör utgå från etablerade principer för säkerhet.

Remisspromemorian: Förslaget hade samma innehåll.

Remissinstanserna: *Svenska Bankföreningen* menar att internrevisionen arbetar utifrån ett riskbaserat synsätt som syftar till att bedöma riskerna i it-verksamheten för hela företaget och att årligen utföra granskningar av olika it-system och it-verksamheten baserat på denna analys. Bankföreningen anser att det är oproportionerligt att peka ut företagets insättningssystem före alla andra system och att internrevisionen fortsatt bör utgå från de risker de ser i den samlade it-verksamheten.

Finansinspektionens skäl: Kravet om att hanteringen av insättningssystem årligen ska granskas av ett företags funktion för internrevision kan komma att innebära att ett företag behöver tillsätta mer resurser än tidigare för internrevisionen av företagets it-verksamhet. Skyddet av informationen och informationens fullständighet och tillförlitlighet är emellertid central för konsumenter och andra kunder. 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. Finansinspektionen har vid sin tillsyn i samband med de fall då insättningsgarantin trätt i kraft även noterat stora brister avseende företagens insättningssystem. Enligt Finansinspektionens uppfattning är det därför väl motiverat att hanteringen av insättningssystem årligen granskas av ett företags funktion för internrevision. De allmänna råden om att ett företag bör följa etablerade principer vid granskningen syftar till att tydliggöra att granskningen bör ske i enlighet med beprövade och vedertagna principer på området. Ett sätt att uppnå detta kan vara genom att vid granskningen utgå från etablerade ramverk eller standarder som exempelvis COBIT eller svensk standard

”riktlinjer för styrning av informationssäkerhet” SS-ISO/IEC 27002 vid granskningen”.

5. Följdändringar i andra föreskrifter och allmänna råd

5.1 Finansinspektionens föreskrifter (FFFS 2007:16) om värdepappersrörelse

Informationssystem och säkerhetsfrågor (3 kap. 15 §)

Finansinspektionens ställningstagande: Det ska framgå av verksamhetsplanen hur it-verksamheten ska vara organiserad. Det ska finnas en översiktlig beskrivning av systemens funktioner och användningsområden.

Om företaget ska hantera order ska det finnas ett flödesschema som visar vilka applikationer som används för orderhantering och en redogörelse för eventuella systemberoende villkor som kan påverka orderhanteringen. Vidare ska det framgå vilka kontroller, exempelvis innehavs- och kreditkontroller, som görs i systemet vid hantering av order.

Det ska också framgå vilka åtgärder ett företag ska vidta i fråga om informationssäkerhet och fysisk säkerhet. När det gäller företagets arbete med informationssäkerhet ska det i verksamhetsplanen finnas en hänvisning till det ledningssystem som företaget ska tillämpa i enlighet med 2 kap. föreskrifterna om hantering av informationssäkerhet, it-verksamhet och insättningssystem.

Allmänna organisatoriska krav (6 kap. 2 §)

Finansinspektionens ställningstagande: Ett värdepappersinstitut ska ha aktuella system och rutiner för att skydda konfidentialitet, riktighet och tillgänglighet i dess information. Systemen och rutinerna ska ta hänsyn till den berörda informationens art.

Remisspromemorian: Innehöll i allt väsentligt samma förslag.

Remissinstanserna: *Myndigheten för samhällsskydd och beredskap (MSB)* föreslår att ordet ”aktuella” ändras till ”uppdaterade” i 6 kap. 2 § för att göra kravet tydligare

Finansinspektionens skäl: Föreskrifterna ska förutom för kreditinstitut gälla även för värdepappersbolag. Finansinspektionen genomför därför vissa mindre ändringar i föreskrifterna om värdepappersrörelse i de delar som specifikt rör frågor som är relaterade till eller täcks av föreskrifterna och allmänna råden om informationssäkerhet, it-säkerhet och insättningssystem.

Till följd av användningen av de på informationssäkerhetsområdet vedertagna begreppen konfidentialitet, riktighet och tillgänglighet i föreskrifterna och

allmänna råden om informationssäkerhet, it-säkerhet och insättningssystem, görs en anpassning av terminologin i 6 kap. 2 § föreskrifterna om värdepappersrörelse. Detta innebär ingen förändring i sak. Finansinspektionen ändrar vidare ordet ”aktuella” till ”uppdaterade” i enlighet med MSB:s förslag. Ändringen innebär ingen förändring i sak.

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

De allmänna råden om ansökan om tillstånd att driva bank- eller finansieringsrörelse (FFFS 2011:50) innehåller bland annat råd om hur en ansökan om tillstånd att driva bank- eller finansieringsrörelse bör vara utformad, samt vilken information en sådan ansökan bör innehålla. Det har i detta regelverksarbete inte funnits möjlighet att göra en allmän översyn av de allmänna råden. Det innebär att de under en övergångsperiod till viss del kommer att innehålla felaktigheter, såsom hänvisningar till författningar som har ändrats.

6. Den nya regleringens konsekvenser

6.1 Allmänt om konsekvenser

Finansinspektionen är enligt förordningen (2007:1244) om konsekvensutredning vid regelgivning skyldig att göra en konsekvensutredning innan nya föreskrifter och allmänna råd beslutas. Remisspromemorian innehöll därför ett avsnitt där Finansinspektionen redogjorde för de potentiella konsekvenser som föreskrifterna kan ge upphov till för bl.a. företagen, samhället och konsumenterna.

Regelrådet avstyrkte förslagen till föreskrifter och allmänna råd eftersom det anser att Finansinspektionens beskrivning av de administrativa kostnaderna är ofullständig och att det saknas uppskattningar av de besparingar som företagen förutspås göra på sikt. *Svenska Bankföreningen* och *Svenska Fondhandlareföreningen* anser att konsekvensutredningen inte uppfyller kraven i förordningen om konsekvenser i regelgivningen, eftersom den inte innehåller några alternativa lösningar som finns för det som Finansinspektionen vill uppnå och vad effekterna blir om någon reglering inte kommer till stånd.

Angående dessa generella invändningar ska sägas att det är mycket svårt och inte alltid ens meningsfullt att kvantifiera kostnader och intäkter för olika typer av aktörer, i synnerhet i ett mer långsiktigt perspektiv. I de flesta fall måste det i slutänden handla om kvalitativa bedömningar. I vissa fall och för vissa aspekter kan en mer kvantifierad bedömning göras, och Finansinspektionen har i samband med remitterandet av föreskriftsförslagen bett remissinstanserna att komma in med en uppskattning av de kostnader som kan uppstå för företagen i

samband med att de inför kraven i föreskrifterna. Inga av remissinstanserna har dock lämnat en sådan kostnadsuppskattning

Detta gäller givetvis också möjligheterna att i kostnads- och intäktstermer jämföra alternativa utformningar av reglerna. Här finns därutöver den aspekten att de föreslagna reglerna i huvudsak innebär en anpassning till internationella normer och praxis av den karaktär som IMF granskar och följer upp. Även om det i dessa fall inte handlar om den typ av tvingande anpassning som en EU-förordning eller EU-direktiv innebär, finns i ett internationellt perspektiv ett värde - förvisso svårkvantifierat - för svensk finansmarknad och för svenska finansföretag att så nära som möjligt ansluta till detta. Med andra ord kan det sägas innebära en kostnad i sig att utforma en alternativ svensk lösning. Omvänt krävs tydliga indikationer på att en egen nationell utformning innebär så stora fördelar att den kostnaden är värd att ta. Finansinspektionen bedömer inte att detta föreligger, och remissinstansernas argument ger heller ingen indikation på att så skulle vara fallet.

6.2 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.

6.3 Konsekvenser för företagen och marknaden

Finansinspektionen har i detta avsnitt gjort vissa uppskattningar av tillkommande kostnader för att införa de nya föreskrifterna.

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.[19] I fallet Barings Bank 1995 uppgick förlusterna till över 15 miljarder kronor.[20] Men även mer vardagliga och mindre spektakulära operativa störningar kan över tid skapa stora kostnader. Om, för att ta ett exempel, internettjänster hos finansiella företag drabbas av upprepade störningar och problem, kan detta dels innebära kostnader för att åtgärda dessa, dels kan det leda till att kunder inte kan använda eller avstår från att använda dessa i grunden effektiva tjänster. Det kan i så fall leda till samhällsekonomiska effektivitetsförluster.

Kostnaderna kopplade till bestämmelserna består både av fasta och löpande kostnader. För ett enskilt företag kan kostnaderna vara beroende av i vilken

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

grad företagets nuvarande processer och metoder är utformade i enlighet med svenska och internationella riktlinjer och standarder. Om befintliga processer och metoder baseras på rekommendationer som motsvarar de föreslagna reglerna bör kostnaden för anpassning till föreskrifterna bli lägre än annars.

För företagen innebär båda de nya föreskrifterna att de 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 i dag uppfyller reglerna kommer således kostnaderna förknippade med förslagen huvudsakligen vara begränsade till att säkerställa detta. För andra företag kan det krävas mer arbete för att ta fram och fastställa nya interna regler och rutiner. En del företag kan också komma att behöva investera i it-system eller rekrytera ytterligare personal.

Som framgår av tidigare avsnitt i promemorian anser 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 kostnader. Nedan redogörs för de materiella, administrativa och finansiella kostnader som de nya reglerna kan komma att föranleda.

6.3.1 Materiella kostnader

De nya reglerna 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 i dag 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 underhållskostnad, medan investeringar i

avancerade analysverktyg med höga krav på flexibilitet kan medföra betydande kostnader för ett företag.

Med antagandet att ett företag som ännu inte infört systemstöd för insamling av uppgifter om incidenter och förluster väljer att göra det, bedöms detta kunna medföra en kostnad av engångskaraktär på mellan 50 000 kronor och 2 miljoner kronor. 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 påpekats tidigare finns det dock inga krav på automatiserade lösningar.

6.3.2 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. Finansinspektionen gör bedömningen att de flesta företag har redan interna regler för hantering av risker som till delar motsvarar de krav som Finansinspektionen ställer gom de nya föreskrifterna. 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 kraven i Finansinspektionens föreskrifter och allmänna råd om styrning, riskhantering och kontroll.

Med antagande att det tar i snitt en arbetsvecka att uppdatera/utveckla en intern regel så att den är anpassad till kraven i föreskrifterna, kan kostnaden för detta beräknas uppgå till cirka 50 000 kronor för ett företag (*40 timmar x 1 300 kronor*). I föreskrifterna anges 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 kronor (*50 000 kronor x 8 interna regler*). Då 259 företag berörs av föreskrifterna uppskattas kostnaden för arbetet med interna regler uppgå till cirka 104 miljoner kronor (*259 företag x 400 000 kronor*).

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 i dag, 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 i dag hos vissa företag.

Finansinspektionen bedömer att behovet av nyanställning för att uppfylla krav i föreskrifterna bör vara begränsat. För ett flertal företag bör det snarare handla om omprioriteringar av arbetsuppgifter för befintlig personal.

Finansinspektionens erfarenhet är att företag redan i dag vidareutbildar sin personal inom riskhantering, till exempel avseende metoder för riskidentifiering, informationssäkerhet, kontinuitetshantering och godkännande av nya produkter. De nya föreskrifterna 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.

6.3.3 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.

6.3.4 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 i högre grad 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 finns inte i fråga om 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 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 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.

6.3.5 Sammanfattning om kostnader

Förlusterna som uppkom under 2012 hos de fyra storbankerna i Sverige och som kan knytas till operativa risker uppgick, enligt uppgifter som Finansinspektionen har begärt in från dessa, till cirka 350 miljoner kronor. För 2013 uppgick förlusterna till omkring 550 miljoner kronor. 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.

Till detta kan läggas kostnaderna för sällan förekommande incidenter av allvarlig art hos finansiella företag. 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 cirka 104 miljoner kronor. Detta är dock endast en typ av kostnad som de föreslagna reglerna kan komma att medföra. Andra kostnader som kan tillkomma är kostnad för personal som ska säkerställa att företagets processer, rutiner och it-system är anpassade till reglerna. Att med säkerhet kvantifiera den totala kostnaden för företagen är mycket svårt då de berörda företagens verksamheter har mycket olika omfattning och komplexitet. För

vissa företag innebär de bestämmelserna sannolikt liten kostnad då företaget i praktiken redan följer dem, medan det för andra företag kan innebära en väsentlig kostnad när bestämmelserna införs.

Vissa remissinstanser har ifrågasatt en del av de beräkningsantaganden som Finansinspektionen använt. Som nämnts är det vanskligt att göra den typen av antaganden, och i synnerhet som bilden torde skilja sig avsevärt mellan olika företag. Varje sådan beräkning måste innebära en grov approximation, och som givetvis kan diskuteras. Finansinspektionen har i samband med remitterandet av föreskiftsförslaget bett remissinstanserna att komma in med en uppskattning av de kostnader som kan uppstå för företagen i samband med att de anpassar sig till kraven i föreskrifterna. Ingen av remissinstanserna har dock hörsammat uppmaningen att lämna en sådan kostnadsuppskattning.

Men även om det totala beloppet hypotetiskt skulle vara dubbelt så stort, dvs. drygt 200 istället för drygt 100 miljoner kronor, kan det sättas i relation till kostnaderna för operativa störningar - som framgått uppgick de fyra storbankernas förluster relaterade till operativa risker år 2012 till minst 350 miljoner kronor. Ett annat jämförelsemått kan vara de fyra storbankernas totala it-kostnader – om man antar att anpassningskostnaden är 200 miljoner kronor blir relationstalet knappt 3 procent, med Finansinspektionens beräkning, det vill säga 100 miljoner kronor hälften, knappt 1,5 procent.[21] Förvisso utgör 100 respektive 200 miljoner kronor mycket aktningsvärda belopp, men Finansinspektionen bedömer likväl att de vinster och fördelar för såväl företagen som för samhället som en bättre hantering av operativa risker kan innebära, gör att detta är väl använda resurser. Enligt Finansinspektionens uppfattning är det mycket osannolikt att en mer precis kostnadsberäkning, som i och för sig skulle vara värdefull, skulle ändra den slutsatsen.

Finansinspektionen anser alltså att kostnader som företagen kommer att få för att förbättra sin riskhantering måste sättas i relation till de risker och kostnader som kan uppstå om nödvändig förbättring i riskhantering inte sker. Trots internationella standarder och riktlinjer saknar idag fortfarande många företag ändamålsenlig dokumentation av sina väsentliga processer och kontroller i dessa, effektiva system för behörighetshantering och har inte testat att deras kontinuitetsplaner kommer att fungera vid avbrott eller störning.
Samtidigt bör ett strukturerat och effektivt riskhanteringsarbete över tiden sänka kostnaderna för operativa förluster. Företagen bör få färre kundklagomål, ökat förtroende 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

[21] It-kostnaderna för storbankerna uppgick 2012 till 6.9 miljarder kronor, personalkostnaderna till 65 miljarder kronor, enligt remissvar från Svenska bankföreningen och Svenska Fondhandlareföreningen

väljer att organisera sin riskhantering. Finansinspektionen bedömer att ett företag genom att införa reglerna i vissa fall även kan reducera sina kostnader för hantering av operativa risker genom att arbeta med riskhantering mer metodiskt.

Som tidigare nämnts kan kostnader för bristande riskhantering bli omfattande både för det enskilda företaget och för dess kunder. 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 sammanfattningsvis att de kostnader som kan uppstå i samband med att företagen stärker sin riskhantering genom införande av reglerna är motiverade.

6.4 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.[22]

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.

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

[22] 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.

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.

6.5 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 föreskrifterna 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.