Finansinspektionens författningssamling

Utgivare: Finansinspektionen, Sverige, www.fi.se
ISSN 1102-7460

FFFS 2014:4
Utkom från trycket
den 17 april 2014

Finansinspektionens föreskrifter och allmänna råd om hantering av operativa risker;

beslutade den 11 april 2014.

Finansinspektionen föreskriver följande med stöd av 5 kap. 2 § 4 förordningen (2004:329) om bank- och finansieringsrörelse och 6 kap. 1 § 9–13 förordningen (2007:572) om värdepappersmarknaden, och lämnar allmänna råd.

1 kap. Tillämpningsområde

1 § Dessa föreskrifter innehåller bestämmelser om hur ett företag ska hantera sina operativa risker.

2 § Föreskrifterna gäller för följande företag:

1. bankaktiebolag,
2. sparbanker,
3. medlemsbanker,
4. kreditmarknadsbolag,
5. kreditmarknadsföreningar, och
6. värdepappersbolag.

3 § För värdepappersbolag gäller dock inte 5 kap. 15–23 §§ samt 6 kap. 4 § 1.

4 § Föreskrifterna innehåller bestämmelser om följande:

– Tillämpningsområde (1 kap.),

– 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.).

Definitioner

5 § I dessa föreskrifter och allmänna råd används samma definitioner som i 1 kap. 3 § Finansinspektionens föreskrifter och allmänna råd (FFFS 2014:1) om styrning, riskhantering och kontroll i kreditinstitut och Finansinspektionens föreskrifter (FFFS 2007:16) om värdepappersrörelse, om inget annat anges i föreskrifterna.

Därutöver betyder

1. *beredskapsplan:* en plan som beskriver de åtgärder som ett företag ska vidta för att hantera allvarliga och omfattande avbrott, störningar eller kriser.

2. *incident*: en händelse som har eller riskerar att få negativ påverkan på företagets verksamhet, tillgångar eller förtroende,

3. *kontinuitetsplan:* en plan som beskriver hur en verksamhet ska upprätthållas i händelse av ett avbrott eller en större verksamhetsstörning,

4. *operativ risk*: detsamma som i artikel 4.1 52 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,[1]

5. *process*: en kedja av sammanhängande aktiviteter som utifrån en viss resursinsats producerar ett resultat, och

6. *återställningsplan:* en plan som beskriver enligt vilka prioriteringar och rutiner ett företag ska återgå till normal verksamhet efter ett avbrott eller en större verksamhetsstörning.

2 kap. Styrning och ansvar

1 § Ett företag ska fastställa en riskaptit för sina operativa risker. Inom ramen för riskaptiten ska företaget även ha limiter för sina operativa risker.

Företaget ska när det fastställer limiter utgå från produkter, tjänster, funktioner, processer och it-system. Limiterna ska kunna vara mätbara genom kvalitativa eller kvantitativa mått. Företaget ska dokumentera riskaptiten och limiterna.

Styrelsen ska besluta om och regelbundet utvärdera och uppdatera riskaptiten för operativa risker om det behövs. Den verkställande direktören ska besluta om och regelbundet utvärdera och uppdatera limiterna för de operativa riskerna om det behövs.

2 § Ett företag ska ha interna regler för sin hantering av operativa risker som anger

1. vilka operativa risker som företaget i huvudsak är exponerat för,

2. dels de metoder och processer som används för att identifiera, mäta och hantera operativa risker som även tar hänsyn till sällan förekommande incidenter av allvarlig art, dels rutiner för att hantera risken för att metoderna kan ge felaktiga resultat, samt

3. företagets rutiner för att fastställa och övervaka riskaptiten och limiterna enligt 1 §.

Om företaget använder risköverföring i sin hantering av operativa risker, ska det ange principerna för detta i de interna reglerna.

Styrelsen ska besluta om de interna reglerna.

[1] Jfr 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 (EUT L 176, 27.6.2013, s. 1, Celex 32013R0575).

Företaget ska när det tillämpar första stycket ta hänsyn till verksamhetens art, omfattning och komplexitet.

Uppdragsavtal

3 § Bestämmelser om uppdragsavtal finns i 9 kap. Finansinspektionens föreskrifter (FFFS 2007:16) om värdepappersrörelse och 10 kap. Finansinspektionens föreskrifter och allmänna råd (FFFS 2014:1) om styrning, riskhantering och kontroll i kreditinstitut.

3 kap. Identifiering och mätning

1 § Ett företag ska identifiera operativa risker i sina produkter, tjänster, funktioner, processer och it-system.

2 § Ett företag ska ha metoder för att identifiera och mäta sina operativa risker. Metoderna ska vara dokumenterade.

Företaget ska när det tillämpar första stycket ta hänsyn till verksamhetens art, omfattning och komplexitet.

3 § Ett företag ska regelbundet mäta de operativa riskerna enligt 1 §, genom att bedöma sannolikheten för att de inträffar och vilka konsekvenserna blir av detta. Företaget ska även fastställa vilka åtgärder det ska vidta för att hantera riskerna.

Riskindikatorer

4 § Ett företag ska fastställa och dokumentera indikatorer och gränsvärden för sina operativa risker som ger en förvarning om när riskerna har ökat.

Företaget ska regelbundet se över och om det behövs uppdatera indikatorerna och gränsvärdena.

Företaget ska när det tillämpar första stycket ta hänsyn till verksamhetens art, omfattning och komplexitet.

Allmänna råd

Exempel på indikatorer som företaget bör beakta är

1. frekventa omorganisationer eller större verksamhetsförändringar,
2. hög personalomsättning,
3. många vakanta tjänster,
4. många kundklagomål,
5. att antalet incidenter har ökat eller typen av incidenter har förändrats, och
6. att funktionen för internrevision har rapporterat om brister i de interna reglerna.

Incidenter

5 § Ett företag ska ha interna regler för att hantera de incidenter som uppstår i verksamheten.

6 § Ett företag ska när det inträffar en incident dokumentera och analysera incidenten. Företaget ska även dokumentera de förluster som har uppstått i samband med denna. Företaget ska ha rutiner för att säkerställa att dessa uppgifter är korrekta. Detta gäller inte om en incident anmäls anonymt.

Företaget ska använda uppgifterna i första stycket när det identifierar och mäter operativa risker enligt 3 §.

4 kap. Rapportering

1 § Ett företag ska i sin rapportering av operativa risker till styrelsen och verkställande direktören ange

1. indikatorer för operativa risker enligt 3 kap. 4 §,
2. överträdelser av riskaptit och risklimiter enligt 2 kap. 1 §, samt
3. allvarliga incidenter.

Företaget ska dessutom minst årligen informera styrelsen om resultatet från tester av beredskapsplaner, kontinuitetsplaner och återställningsplaner.

Företaget ska när det tillämpar första och andra styckena ta hänsyn till verksamhetens art, omfattning och komplexitet.

5 kap. Hantering av operativa risker i verksamheten

Processer

1 § Ett företag ska fastställa och i en förteckning ange vilka processer i verksamheten som är av väsentlig betydelse.

Förteckningen ska regelbundet ses över och uppdateras om det behövs.

2 § Ett företag ska dokumentera processerna enligt 1 § och utse en ansvarig person eller funktion för varje sådan process.

3 § Ett företag ska i interna regler ange hur det ska dokumentera processerna enligt 1 § och hur operativa risker i dessa ska hanteras.

Företaget ska när det tillämpar första stycket ta hänsyn till verksamhetens art, omfattning och komplexitet.

Allmänna råd

Företaget bör i processdokumentationen enligt 2 § beskriva

1. vilka regler som påverkar processens utformning,
2. processens huvudsakliga aktiviteter och deras samband (flödesschema),
3. vilken information som används i aktiviteterna enligt 2,
4. de krav som ställs på kvalitet i informationen enligt 3,
5. vilka it-system som stödjer processen,
6. när kontroll görs och beslut fattas i processen,
7. intressenter till processen, t.ex. personal, kunder, myndigheter, underleverantörer och andra företag, samt
8. processens resultat, t.ex. en tjänst, produkt eller en annan uteffekt.

4 § Ett företag ska ha rutiner för att analysera om det finns aktiviteter i processerna enligt 1 § där det finns risk för betydande förluster på grund av t.ex. misstag, manipulering av information samt möjlighet att dölja felbedömningar och förluster.

Om företaget identifierar sådana aktiviteter ska det införa nödvändiga kontroller i processerna.

Rutinerna enligt första stycket ska dokumenteras.

Företaget ska när det tillämpar första och andra styckena ta hänsyn till verksamhetens art, omfattning och komplexitet.

Personal

5 § Ett företag ska ha rutiner för hur det hanterar operativa risker i fråga om sin personal, där det framgår hur företaget

1. kontrollerar nödvändiga uppgifter och särskilt beaktar risken för intressekonflikter i samband med att företaget anställer ny personal,

2. ser till att det har tillräckligt med personal i förhållande till arbetsuppgifterna,

3. dels utvärderar om det har personal med en sådan kompetens eller som fyller en sådan funktion att de är svåra att ersätta med kort varsel, dels utser ersättare för sådan personal,

4. fastställer krav på kompetens och kunskap för personalen samt ser till att deras kompetens och kunskap upprätthålls,

5. fastställer och uppdaterar befattningsbeskrivningar, mandat och limiter,

6. hanterar den tystnadsplikt som regleras i 1 kap. 10 § lagen (2004:297) om bank- och finansieringsrörelse och 1 kap. 11 § värdepappersmarknadslagen (2007:528), samt

7. identifierar och hanterar operativa risker som kan uppstå i samband med att personalen internt byter arbetsuppgifter eller organisatorisk enhet.

Företaget ska när det tillämpar första stycket ta hänsyn till verksamhetens art, omfattning och komplexitet.

Legala risker

6 § Ett företag ska i interna regler ange hur det hanterar legala risker. De interna reglerna ska ange på vilket sätt företaget

1. säkerställer att verksamheten följer lagar, förordningar och andra regler,
2. säkerställer och följer upp att ingångna avtal eller andra rättshandlingar är korrekta och giltiga,
3. arkiverar avtal och andra rättshandlingar, samt
4. hanterar och följer upp rättsliga processer.

De interna reglerna enligt första stycket ska även ange vilken person eller funktion som ansvarar för hanteringen av 1–4.

Säkerhetsarbete

7 § Ett företag ska ha interna regler för säkerhetsarbete som innehåller uppgifter om vilka tillgångar och värden som ska skyddas. Företaget ska ange dels vilka åtgärder det ska vidta för att skydda dessa, dels hur omfattande åtgärderna ska vara.

Företaget ska när det tillämpar första stycket ta hänsyn till verksamhetens art, omfattning och komplexitet.

Allmänna råd

Företaget bör i säkerhetsarbetet använda scenarion eller simuleringar för att öka kunskapen om hur olika typer av hot, oegentligheter och brottsliga handlingar kan uppstå i företagets verksamhet.

8 § Bestämmelser om informationssäkerhet finns i 2 kap. Finansinspektionens föreskrifter och allmänna råd (FFFS 2014:5) om informationssäkerhet, it-verksamhet och insättningssystem.

It-system

9 § Bestämmelser om hur ett företag ska hantera it-system finns i 3 kap. Finansinspektionens föreskrifter och allmänna råd (FFFS 2014:5) om informationssäkerhet, it-verksamhet och insättningssystem.

Process för godkännande

10 § 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.

Företaget ska när det tillämpar första stycket ta hänsyn till verksamhetens art, omfattning och komplexitet.

11 § Ett företag ska i interna regler beskriva processen för godkännande enligt 10 §. De interna reglerna ska även ange

1. vad företaget avser med nya eller väsentligt förändrade befintliga produkter, tjänster, marknader, processer, it-system och större förändringar i företagets verksamhet och organisation, samt

2. vilka funktioner och enheter som ska delta i processen.

Företaget ska när det tillämpar första stycket ta hänsyn till verksamhetens art, omfattning och komplexitet när det tar fram de interna reglerna.

12 § Ett företag ska se till att följande moment finns med i processen för godkännande enligt 10 §:

1. kontroll av att gällande regler följs,

2. analys av om företagets risknivåer kan öka eller om nya risker kan uppstå och om detta kan påverka företagets kapitalbehov,

3. kontroll av att det finns tillräckligt med personal och tillgång till kompetens, interna regler, verktyg och processer i affärsenheter samt stöd- och kontrollfunktioner för att kunna förstå och övervaka riskerna, samt

4. dokumentation av beslut om godkännande där de överväganden framgår som legat till grund för beslutet.

13 § Om det inte anges i de interna reglerna enligt 11 § 1 att processen enligt 10 § ska tillämpas ska funktionen för riskontroll avgöra detta.

14 § 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.

Kontinuitetshantering

15 § Ett företag ska i interna regler för kontinuitetshantering ange

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

2. ansvariga (roller och befattningar) för att styra verksamheten och för att besluta om åtgärder vid ett avbrott eller en större verksamhetsstörning, samt

3. principer för att hantera och besluta om åtgärder beroende på typen och omfattningen av avbrott eller en större verksamhetsstörning.

Företaget ska när det tillämpar första stycket ta hänsyn till verksamhetens art, omfattning och komplexitet.

Den verkställande direktören ska besluta om de interna reglerna.

16 § Ett företag ska för varje process enligt 5 kap. 1 § fastställa den längst tillåtna tiden för avbrott.

Analys av konsekvenser och planering för återställning

17 § Ett företag ska regelbundet analysera konsekvenserna av sådana avbrott eller större verksamhetsstörningar som kan inträffa i företagets verksamhet samt i den verksamhet som företaget har uppdragit åt någon annan.

18 § Konsekvensanalysen enligt 17 § ska genomföras på alla affärsenheter och stödfunktioner och ta hänsyn till deras beroende av varandra. Ett företag ska använda analysen som underlag för att

1. fastställa företagets prioriteringar och mål för att återgå till normal verksamhet efter ett avbrott eller en större verksamhetsstörning, samt

2. ta fram beredskapsplaner, kontinuitetsplaner och återställningsplaner.

Planerna enligt 2 ska vara dokumenterade.

19 § 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.

Allmänna råd

Om företaget har ett alternativt it-driftställe bör det se till att detta inte är beroende av samma fysiska infrastruktur som det huvudsakliga driftstället, och att data samt säkerhetskopior som förvaras på de båda driftställena inte kan förstöras samtidigt.

Kommunikation och utbildning

20 § Ett företag ska ha rutiner för att hantera sin interna och externa kommunikation i samband med ett avbrott eller en större verksamhetsstörning. Företaget ska när det planerar kommunikationen även ta hänsyn till om ett avbrott eller en störning kan få betydande konsekvenser för verksamheten hos dotterbolag eller filialer, eller på annat sätt kan påverka det finansiella systemet.

21 § Ett företag ska regelbundet utbilda och informera sin personal om hur den ska använda beredskapsplaner, kontinuitetsplaner och återställningsplaner.

Uppdatering och test av planer

22 § Ett företag ska regelbundet uppdatera och testa sina beredskapsplaner, kontinuitetsplaner och återställningsplaner så att de är anpassade till verksamheten och prioriteringarna för att återgå till normal verksamhet enligt 18 §.

Företaget ska utse en ansvarig person eller funktion för uppdatering och test av varje sådan plan.

23 § Ett företag ska i de interna reglerna om kontinuitetshantering enligt 15 § fastställa

1. vilka typer av tester det ska utföra enligt 22 §, samt
2. hur ofta testerna ska utföras.

Beredskapsplaner, kontinuitetsplaner och återställningsplaner för processer enligt 5 kap. 1 § samt de it-system som stödjer dessa processer ska testas minst årligen.

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

1 § Bestämmelserna i detta kapitel ska, utöver det som anges i 1–5 kap., tillämpas på företag som har tillstånd att tillhandahålla investeringstjänster och utföra investeringsverksamheter enligt 2 kap. 1 § 2–3 lagen (2007:528) om värdepappersmarknaden och av de företag som driver valutahandel enligt 7 kap. 1 § 12 lagen (2004:297) om bank- och finansieringsrörelse.

Åtskillnad av arbetsuppgifter

2 § 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.

Personal

3 § Ett företag ska se till att personal som hanterar affärstransaktioner under minst tio arbetsdagar i följd under en tolvmånadersperiod inte har möjlighet att

1. initiera och genomföra affärstransaktioner,
2. godkänna eller bekräfta affärstransaktioner, eller
3. hantera betalningar kopplade till affärstransaktioner.

Transaktionshantering

4 § Ett företag ska se till att

1. det finns en fullständig och dokumenterad verifieringskedja för varje transaktion och att verifieringskedjan säkerställer spårbarhet som gör uppföljning möjlig per handlare,

2. det finns dokumenterade rutiner och kontroller i hela kedjan från öppnandet av en affärsrelation till avveckling av utförda transaktioner,

3. villkor för transaktionen dokumenteras och bekräftas innan handel påbörjas,

4. personal som initierar och genomför affärstransaktioner så snart som möjligt efter ett transaktionsavslut, lämnar nödvändig information och dokumentation till stödfunktionerna så att de kan stämma av, bekräfta, avveckla och följa upp transaktionen,

5. det finns fastställda rutiner för att hantera och rapportera felaktigt utförda transaktioner,

6. det dels finns fastställda rutiner för att hantera och rapportera obekräftade affärer, dels följa upp dessa dagligen, samt

7. dagligen stämma av transaktioner, likvider och positioner.

Avstämningen enligt 7 ska även omfatta ändringar och makuleringar.

Hantering av säkerheter

5 § Ett företag ska ha rutiner för att hantera och kontrollera säkerheterna i samband med transaktioner och positioner.

6 § Ett företag ska se till att det finns fastställda rutiner för kontroll av utrymme inom motpartslimiter innan dessa utnyttjas vid handel.

Övervakning och kontroll

7 § Ett företag ska vid väsentliga avvikelser eller orimliga resultat vid handel analysera om dessa är orsakade av misstag, oegentligheter eller andra händelser i verksamheten.

8 § Ett företag ska löpande granska och stämma av sina samtliga konton.

9 § Ett företag ska kontrollera värdet på sina nettopositioner och de transaktioner som ger upphov till dessa.

10 § Ett företag ska fastställa och regelbundet följa upp limiter för sina positioner. Företaget ska sätta limiterna så att det är möjligt att följa upp och kontrollera dem.

11 § Ett företag ska minst en gång i kvartalet, kontrollera att behörigheter till de it-system som används i verksamheten är begränsade till behov utifrån tilldelade arbetsuppgifter.

Dessa föreskrifter och allmänna råd träder i kraft den 1 juni 2014.

MARTIN ANDERSSON

Agnieszka Arshamian