

Observera att denna konsoliderade version är en sammanställning, och att den tryckta författningen är den officiellt giltiga. En konsoliderad version är en fulltextversion där alla ändringar har införts i grundförfattningen.



Finansinspektionens författningssamling

Utgivare: Tillförordnad chefsjurist Sophie Degenne, Finansinspektionen, Sverige,
www.fi.se
ISSN 1102-7460

FFFS 2014:1

Finansinspektionens föreskrifter och allmänna råd om styrning, riskhantering och kontroll i kreditinstitut

Konsoliderad elektronisk utgåva

Senast uppdaterad: 2025-03-24

Observera att endast den tryckta utgåvan gäller vid rättstillämpning

Beslutade: 2014-02-17

Ikraftträdande: 2014-04-01

Ändringar: FFFS 2014:30, FFFS 2016:8, FFFS 2017:8, FFFS 2021:21,
FFFS 2024:28

1 kap. Tillämpningsområde och definitioner

Tillämpningsområde

1 § Dessa föreskrifter gäller för

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

Föreskrifterna ska också tillämpas på värdepappersrörelsen i dessa företag med undantag av bestämmelserna i

- 2 kap. 1, 8 och 9 §§,
- 3 kap. 3 och 4 §§,
- 4 kap. 3–6 §§,
- 5 kap. 1–3 §§,
- 8 kap. 1 § och 3 § 2, 3, 6 och 7,
- 9 kap. 4 § och 5 § 9, och
- 10 kap.

Företaget ska i sin värdepappersrörelse inte tillämpa 6 kap. 6 § 4 på funktionen för regelefterlevnad. Bestämmelser om funktionen för regelefterlevnads oberoende finns i artikel 22.3 i den delegerade förordningen till Mifid 2.

Föreskrifterna ska, i enlighet med vad som gäller enligt 3 kap. 4 § lagen (2014:968) om särskild tillsyn över kreditinstitut och värdepappersbolag, tillämpas på grupp- eller undergruppsnivå. (FFFS 2024:28)

1 a § Bestämmelserna i 2 och 3 kap. gäller inte för hantering av IKT-risker enligt kapitel II i Dora-förordningen.

Bestämmelserna i 5 kap. gäller inte för hantering av IKT-risker enligt kapitel II–V i Dora-förordningen.

Bestämmelserna i 10 kap. gäller inte för sådana uppdragsavtal som omfattas av kapitel V i Dora-förordningen. (FFFS 2024:28)

Föreskrifternas innehåll

2 § I föreskrifterna finns bestämmelser om följande:

- Allmänna organisatoriska krav (2 kap.),
- Styrelsens och den verkställande direktörens ansvar (3 kap.),
- Etiska regler (4 kap.),
- Riskhantering (5 kap.),
- Kontrollfunktioner (6 kap.),
- Funktion för riskkontroll (7 kap.),
- Regelefterlevnad (8 kap.),
- Funktion för internrevision (9 kap.), och
- Uppdragsavtal (10 kap.).

Definitioner

3 § I dessa föreskrifter och allmänna råd ska termer och uttryck ha följande betydelse.

1. *Den delegerade förordningen till Mifid 2*: kommissionens delegerade förordning (EU) 2017/565 av den 25 april 2016 om komplettering av Europaparlamentets och rådets direktiv 2014/65/EU vad gäller organisatoriska krav och villkor för verksamheten i värdepappersföretag, och definitioner för tillämpning av det direktivet.

2. *Dora-förordningen*: Europaparlamentets och rådets förordning (EU) 2022/2554 av den 14 december 2022 om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014, (EU) nr 909/2014 och (EU) 2016/1011.

3. *EES*: Europeiska ekonomiska samarbetsområdet.

4. *Ersättningskommitté*: detsamma som i Finansinspektionens föreskrifter (FFFS 2011:1) om ersättningssystem i kreditinstitut.
5. *Funktion*: en enhet eller en avdelning som består av en eller flera personer med uppdrag att utföra en eller flera uppgifter inom verksamheten.
6. *Interna regler*: policy- och styrdokument, riktlinjer, instruktioner eller andra skriftliga dokument genom vilka ett företag styr sin verksamhet.
7. *Kontrollfunktion*: en funktion för riskkontroll, regelefterlevnad eller internrevision.
8. *Limit*: en fastställd gräns för riskexponering som avser t.ex. en viss kund, kundgrupp, marknad eller produkt.
9. *Ramverk för riskhantering*: företagets strategier, processer, rutiner, interna regler, limiter, kontroller och rapporteringsrutiner som utgör en ram för företagets riskhantering.
10. *Riskaptit*: en nivå och inriktning på företagets risker som kan accepteras för att uppnå företagets strategiska mål.
11. *Riskexponering*: ett mått på den risk som ett företag är exponerat för vid en viss tidpunkt.
12. *Riskkultur*: yrkesmässiga värderingar, attityder och beteenden som har avgörande betydelse för hur ett företag hanterar sina risker.
13. *Riskstrategi*: en strategi för att ta på sig, styra och ha kontroll över de risker som företaget är eller kan bli exponerat för.
14. *Tillsynsförordningen*: Europaparlamentets och rådets förordning (EU) nr 575/2013 av den 26 juni 2013 om tillsynskrav för kreditinstitut och om ändring av förordning (EU) nr 648/2012.
15. *Uppdragsavtal*: ett avtal mellan ett företag och en uppdragstagare genom vilket uppdragstagaren utför en process, en tjänst eller en verksamhet som företaget annars självt skulle ha utfört.
16. *Verkställande ledning*: detsamma som i Finansinspektionens föreskrifter (FFFS 2011:1) om ersättningssystem i kreditinstitut. (FFFS 2024:28)

2 kap. Allmänna organisatoriska krav

1 § Ett företag ska se till att

1. ha en ändamålsenlig och överblickbar organisationsstruktur med en tydlig fördelning av funktioner och ansvarsområden som dels säkerställer att företaget styrs effektivt och sunt, dels gör det möjligt för Finansinspektionen att utöva en effektiv tillsyn,
2. ha aktuella och dokumenterade beslutsrutiner som tydligt anger rapporteringsvägar,
3. varje relevant befattnings ansvar och arbetsuppgifter är dokumenterade i en befattningsbeskrivning,

4. all personal är informerad om vilka rutiner som de ska följa för att kunna fullgöra sina skyldigheter,
5. ha aktuella och ändamålsenliga interna kontrollmekanismer som innefattar kontrollfunktioner, it-system och processer, för att säkerställa att beslut och rutiner följs på alla nivåer inom företaget,
6. ha personal med den kompetens och kunskap som krävs för att de ska kunna fullgöra sina arbetsuppgifter,
7. ha en aktuell och ändamålsenlig intern och extern rapportering och spridning av information i företaget,
8. bevara relevanta uppgifter som avser verksamheten och den interna organisationen i minst fem år, och
9. om en person arbetar inom flera funktioner, detta inte hindrar honom eller henne från att fullgöra sina uppgifter på ett korrekt sätt.

Företaget ska när det tillämpar första stycket ta hänsyn till verksamhetens art, omfattning och komplexitet, och arten på och omfattningen av företags tjänster och verksamhet.

För en grupp eller en enhet med anställda som utför identiska arbetsuppgifter kan en befattningsbeskrivning enligt första stycket 3 omfatta hela den aktuella gruppen eller enheten.

2 § Har upphävts genom (FFFS 2024:28).

3 § Ett företag ska ha en dokumenterad riskaptit som omfattar företagets alla slag av risker.

Styrelsen ska besluta om företagets riskaptit och regelbundet utvärdera riskaptiten och uppdatera den om det behövs.

4 § Ett företag ska ha en dokumenterad riskstrategi.

Styrelsen ska besluta om företagets riskstrategi och regelbundet utvärdera riskstrategin och uppdatera den om det behövs.

5 § Ett företag ska ha interna regler för styrning och kontroll av sin organisation och verksamhet som är anpassade till verksamhetens art, omfattning och komplexitet.

Styrelsen ska besluta om de interna reglerna.

6 § Ett företag ska ha it-system och rapporteringsrutiner som säkerställer att information om dess verksamhet och riskexponering är aktuell och relevant samt att den externa rapporteringen är tillförlitlig, aktuell, fullständig och att den rapporteras i tid. (FFFS 2014:30)

7 § Ett företag ska ha förmåga att så snart som möjligt samla in och automatiskt sammanställa data för företagets väsentliga och mätbara risker. De it-system som stödjer sammanställningen ska vara flexibla och kunna möta olika analysbehov. Riskdata ska kunna sammanställas åtminstone vid krissituationer, stresstester samt på begäran från Finansinspektionen.

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

Allmänna råd

Riskdatan bör kunna sammanställas per verksamhetsområde, juridisk person, tillgångsslag, typ av motpart, region och andra relevanta grupperingar på ett sätt som gör det möjligt att identifiera och rapportera riskexponeringar, riskkoncentrationer och riskförändringar.

8 § Ett företag ska ha interna regler och rutiner för sin redovisning och riskrapportering som gör det möjligt att på begäran från Finansinspektionen, inom rimlig tid, lämna finansiella rapporter som dels ger en rättvisande bild av företags finansiella ställning, dels överensstämmer med tillämplig redovisningsstandard, redovisningsregler samt legala krav för riskrapportering.

Styrelsen eller den verkställande direktören ska besluta om de interna reglerna.

9 § Ett företag ska ha en väl fungerande kontinuitetshantering som säkerställer att företagets viktigaste information bevaras samt att verksamheten upprätthålls vid ett avbrott eller en större verksamhetsstörning.

10 § Ett företag ska säkerställa att det har rutiner för åtskillnad av arbetsuppgifter och förebyggande av intressekonflikter. Företaget ska även se till att ingen person ensam handlägger en transaktion genom hela behandlingskedjan.

Företaget behöver inte uppfylla det som anges i första stycket andra meningen om transaktionen är obetydlig. (FFFS 2014:30)

11 § Ett företag ska övervaka och regelbundet utvärdera de system, interna kontrollmekanismer och rutiner som anges i 1–10 §§, för att säkerställa att de är effektiva och ändamålsenliga. Företaget ska dessutom vidta lämpliga åtgärder för att korrigera eventuella brister.

12 § Ett företag ska avsätta tillräckligt med resurser för att utbilda styrelseledamöterna. (FFFS 2014:30)

13 § Ett företag ska när det tillsätter styrelseledamöter beakta en bred uppsättning egenskaper och kunskaper och för detta ändamål ha en policy för att främja mångfald i styrelsen. (FFFS 2014:30)

14 § Ett företag ska på sin webbplats förklara hur det organiserar och styr verksamheten. Företaget ska på webbplatsen även förklara hur styrelsen, styrelseledamöterna och den verkställande direktören uppfyller kraven på tillräcklig kunskap, insikt, erfarenhet och lämplighet.

Om företaget inte har en webbplats ska det kunna tillhandahålla informationen på annat sätt till allmänheten. (FFFS 2014:30)

3 kap. Styrelsens och den verkställande direktörens ansvar

Styrelsens ansvar och uppgifter

1 § När styrelsen fastställer företagets strategier ska den ta hänsyn till företagets långsiktiga finansiella intressen, de risker företaget exponeras för och kan förväntas komma att exponeras för, samt det kapital som krävs för att täcka företagets risker.

2 § Styrelsens ledamöter ska ha god kännedom om och förståelse för företagets organisationsstruktur och processer för att kunna säkerställa att dessa är förenliga med företagets beslutade strategier. Ledamöterna ska vara väl insatta i och ha god kännedom om företagets verksamhet samt arten och omfattningen av dess risker.

Styrelsens och den verkställande direktörens ansvar och uppgifter

3 § Styrelsen ska regelbundet, minst årligen, utvärdera och om det behövs uppdatera de interna regler som den har beslutat om. Den verkställande direktören ska regelbundet, minst årligen, utvärdera de interna regler som den beslutat om och om det behövs uppdatera dessa.

Därutöver ska styrelsen eller den verkställande direktören regelbundet se över och bedöma effektiviteten i företagets organisationsstruktur, rutiner, åtgärder, metoder m.m. som företaget har beslutat för att följa lagar och andra författningar som reglerar företagets tillståndspliktiga verksamhet. Styrelsen eller den verkställande direktören ska även vidta lämpliga åtgärder för att korrigera eventuella brister i dessa.

4 § Styrelsen eller den verkställande direktören ska regelbundet utvärdera om företaget kontrollerar och hanterar sina risker på ett effektivt och ändamålsenligt sätt.

4 kap. Etiska regler

1 § Ett företag ska driva sin verksamhet på ett etiskt ansvarsfullt och professionellt sätt samt upprätthålla en sund riskkultur. Bestämmelser om intressekonflikter finns i 2–6 §§ och bestämmelser om ersättningspolicy i 2–4 kap. Finansinspektionens föreskrifter (FFFS 2011:1) om ersättningssystem i kreditinstitut, värdepappersbolag och fondbolag med tillstånd för diskretionär portföljförvaltning. Allmänna råd om etiska riktlinjer finns i Finansinspektionens allmänna råd (FFFS 1998:22) om riktlinjer för hantering av etiska frågor hos institut som står under inspektionens tillsyn.

Intressekonflikter i verksamheten

2 § har upphävts genom (FFFS 2017:8)

3 § Ett företag ska identifiera och hantera de intressekonflikter som finns eller kan förväntas komma att uppstå i verksamheten.

4 § Ett företag ska ha interna regler som anger hur företaget hanterar intressekonflikter enligt 3 §. De interna reglerna ska vara lämpliga med hänsyn till företagets storlek och organisation samt till verksamhetens art, omfattning och komplexitet.

Styrelsen ska besluta om de interna reglerna.

5 § Om ett företag ingår i en konsoliderad situation enligt artikel 18 i tillsynsförordningen, ska det i de interna reglerna om intressekonflikter enligt 4 § också ta hänsyn till de omständigheter som till följd av strukturen eller verksam-

heten i andra företag i gruppen, kan ge upphov till en intressekonflikt. (FFFS 2014:30)

6 § Ett företag ska i de interna reglerna för intressekonflikter enligt 4 §

1. identifiera vilka omständigheter som utgör eller kan förväntas komma att ge upphov till en intressekonflikt som medför en väsentlig risk för att en eller flera kunders intressen påverkas negativt med hänsyn till företagets produkter och tjänster, och

2. ange vilka rutiner som ska tillämpas och vilka åtgärder som ska vidtas för att hantera sådana konflikter.

5 kap. Riskhantering

1 § Ett företag ska ha ett ramverk för riskhantering som innehåller de strategier, processer, rutiner, interna regler, limiter, kontroller och rapporteringsrutiner som behövs för att säkerställa att företaget löpande kan identifiera, mäta, styra, internt rapportera och ha kontroll över de risker som det är eller kan förväntas komma att bli exponerat för.

2 § Ramverket för riskhantering enligt 1 § ska vara väl integrerat i företagets organisations- och beslutsstruktur samt avse samtliga väsentliga risker i företaget. Företagets affärsenheter ansvarar för att utföra den dagliga riskhanteringen.

3 § Ett företag ska ha interna regler för sin riskhantering.

Styrelsen ska besluta om de interna reglerna.

4 § Ett företag ska när det inför nya, eller väsentligt förändrade, produkter, tjänster, marknader och processer, och vid större förändringar i företagets verksamhet och organisation, hantera de risker som kan uppstå i samband med detta på ett effektivt och ändamålsenligt sätt. (FFFS 2024:28)

Riskrapportering

5 § Ett företag ska ha en rutin för att regelbundet rapportera de risker som finns eller kan förväntas uppstå i verksamheten till styrelsen och riskutskottet, om ett sådant har inrättats, den verkställande direktören, och övriga funktioner som behöver ha informationen, så att de får tillförlitliga, aktuella och fullständiga rapporter i rätt tid.

Styrelsen och riskutskottet, om ett sådant har inrättats, ska fastställa arten, mängden, formatet och frekvensen på riskinformationen som de ska få ta emot. (FFFS 2014:30)

Riskkultur

6 § Ett företag ska ha en gemensam och sund syn på risktagande som baseras på en förståelse för samtliga risker som företaget kan exponeras för, samt hur dessa tas om hand i företaget. En sådan riskkultur ska ta hänsyn till företagets beslutade riskapitit. Företaget ska löpande informera och utbilda berörd personal så att den har relevant kunskap om företagets ramverk för riskhantering.

Limiters och mandat

7 § Ett företag ska sätta tydliga gränser (limiter och mandat) för den som ska fatta beslut inom ramen för företagets riskaptit.

8 § Ett företag ska ha rutiner för att övervaka och kontrollera att de limiter och mandat som beslutats enligt 7 § följs.

9 § Ett företag ska ha interna regler för hur det hanterar överträdelser av limiter och mandat enligt 7 §. Företaget ska även ha rutiner för hur det ska utvärdera en överträdelse samt informera de funktioner som ska vidta åtgärder enligt de interna reglerna. Funktionen för riskkontroll ska utvärdera överträdelsen samt informera berörda funktioner om resultatet.

Riskbedömning

10 § När ett företag identifierar, bedömer och mäter risker ska det utföra framåt- och bakåtblickande analyser.

11 § Ett företag ska när det bedömer företagets risker göra en egen kritisk granskning av dessa och inte enbart förlita sig på externa bedömningar.

Riskutskott

12 § Ett företag som är betydande i fråga om storlek, intern organisation och verksamhetens art, omfattning och komplexitet ska se till att styrelsen har ett riskutskott. Riskutskottet ska bestå av ledamöter i styrelsen som inte ingår i företagets verkställande ledning. Riskutskottets ledamöter ska ha lämpliga kunskaper och färdigheter för att kunna förstå och övervaka företagets riskstrategi och riskaptit. *(FFFS 2016:8)*

13 § Riskutskottet ska fungera som rådgivare för styrelsen när det gäller företagets samlade nuvarande och framtida riskaptit och riskstrategi och bistå styrelsen när den övervakar den verkställande ledningens genomförande av strategin. Styrelsen ska behålla det övergripande riskansvaret. *(FFFS 2016:8)*

14 § Riskutskottet ska se till att priset på skulder och tillgångar som erbjuds kunderna beaktar företagets affärsmodell och riskstrategi. Om priserna inte korrekt återspeglar riskerna i enlighet med affärsmodellen och riskstrategin ska riskutskottet ta fram en åtgärdsplan för styrelsen. *(FFFS 2016:8)*

15 § För att bistå vid upprättandet av en sund ersättningspolicy och ersättningspraxis ska riskutskottet, utan att det påverkar de uppgifter och det ansvar som företagets ersättningskommitté har, undersöka om incitamenten i ersättningssystemet tar hänsyn till risk, kapital, likviditet samt sannolikheten och tidpunkten för företagets resultat. *(FFFS 2016:8)*

6 kap. Kontrollfunktioner

Generella krav på kontrollfunktionerna

1 § Ett företag ska ha en funktion för riskkontroll, en funktion för regelefterlevnad och en funktion för internrevision. Kontrollfunktionerna ska vara organisatoriskt

skilda från varandra. I små företag med mindre komplex verksamhet kan funktionen för riskkontroll och funktionen för regelefterlevnad vara kombinerad.

2 § Varje kontrollfunktions arbete ska regleras av interna regler. De interna reglerna ska ange varje kontrollfunktions ansvar, uppgifter och rutiner för rapportering.

Styrelsen ska besluta om de interna reglerna.

3 § En kontrollfunktion enligt 1 § ska ha de resurser som krävs samt tillgång till den information som behövs för att kunna fullgöra sina uppgifter. En sådan funktion ska ha personal med den kunskap som krävs samt de befogenheter som behövs för att den ska kunna fullgöra sina uppgifter.

4 § Ett företag ska se till att personalen i en kontrollfunktion enligt 1 § löpande utbildas för att hålla kunskapen aktuell.

5 § En kontrollfunktion enligt 1 § ska ha ändamålsenliga it-system och stöd till sitt förfogande.

Oberoende

6 § En kontrollfunktion enligt 1 § ska vara oberoende. För att en kontrollfunktion ska anses oberoende ska

1. personalen i kontrollfunktionen inte utföra några uppgifter som ingår i verksamheten som de ska övervaka och kontrollera,
2. den organisatoriskt vara skild från de funktioner och områden som den ska övervaka och kontrollera,
3. den ansvarige för kontrollfunktionen regelbundet rapportera direkt till styrelsen och närvara vid styrelsens sammanträden då respektive funktions ansvarsområde eller rapporter behandlas, och
4. metoden för att fastställa ersättning till personalen i kontrollfunktionen inte vara utformad så att den äventyrar eller kan förväntas komma att äventyra personalens objektivitet.

Rapportering

7 § En kontrollfunktion enligt 1 § ska regelbundet, minst årligen, rapportera om väsentliga brister och risker till styrelsen, riskutskottet, om ett sådant har inrättats, och den verkställande direktören. Rapporterna ska följa upp tidigare rapporterade brister och risker och redogöra för varje ny identifierad väsentlig brist och risk. En konsekvensanalys och en rekommendation till åtgärder ska även ingå i rapporten. Styrelsen, riskutskottet och den verkställande direktören ska så snart som möjligt vidta lämpliga åtgärder med anledning av kontrollfunktionens rapport. (FFFS 2014:30)

8 § Ett företag ska ha rutiner för att regelbundet följa upp vilka åtgärder som det vidtar med anledning av en kontrollfunktions rapport.

7 kap. Funktion för riskkontroll

1 § Företagets funktion för riskkontroll enligt 6 kap. 1 § ska vara direkt underställd den verkställande direktören eller i förekommande fall företagets riskchef. Ett företag som har flera funktioner för riskkontroll ska ha en central funktion för riskkontroll som ansvarar för att sammanställa, analysera och rapportera företagets samtliga risker.

2 § Funktionen för riskkontroll ska bestå av personer med tillräcklig kunskap om dels metoder och rutiner för att hantera risker, dels marknader och produkter för att kunna lämna relevant och oberoende information, analyser och expertutlåtanden om företagets risker.

3 § Funktionen för riskkontroll ska

1. dels kontrollera att alla väsentliga risker som företaget exponeras för eller kan förväntas komma att exponeras för identifieras och hanteras av berörda funktioner, dels identifiera risker som uppstår på grund av brister i företagets riskhantering, dels kontrollera att varje affärsenhet övervakar samtliga för affärsenheten väsentliga risker på ett effektivt sätt,

2. övervaka och kontrollera företagets riskhantering,

3. kontrollera och analysera företagets väsentliga risker och utvecklingen av dessa samt identifiera dels nya risker som kan uppstå till följd av förändrade förutsättningar, dels risker som härrör från graden av komplexitet i företagets legala struktur,

4. se till att information om företagets risker regelbundet lämnas till styrelsen samt regelbundet, dock minst kvartalsvis, rapportera sin bedömning såväl skriftligt som muntligt till styrelsen,

5. när företaget lägger fram förslag eller fattar beslut som medför att företagets risker kan öka väsentligt, bedöma om dessa är förenliga med företagets beslutade riskaptit,

6. när företaget tar fram eller ändrar sin riskstrategi och riskaptit, lämna all relevant information som kan utgöra underlag för beslut i dessa frågor samt bedöma föreslagen riskstrategi och lämna en rekommendation innan beslut fattas,

7. kontrollera att relevanta interna regler, processer och rutiner enligt 5 kap. 1 § följs, att de är ändamålsenliga och effektiva samt föreslå ändringar i dessa om det behövs,

8. identifiera, kontrollera och rapportera risker för fel i företagets antaganden och bedömningar som ligger till grund för företagets finansiella rapportering, och

9. innan företaget beslutar om nya, eller väsentligt förändrade, produkter, tjänster, marknader, processer och it-system samt vid större förändringar i företagets verksamhet och organisation utvärdera risker med dessa samt utvärdera hur dessa kan förväntas komma att påverka företagets sammanvägda risk.

Riskchef

4 § Ett företag ska om det är lämpligt och rimligt med hänsyn till verksamhetens art, omfattning och komplexitet utse en riskchef, som ska ansvara för funktionen för riskkontroll och bedöma om företagets ramverk för riskhantering är effektivt och ändamålsenligt. Riskchefen ska vara direkt underställd den verkställande

direktören och ska rapportera direkt till denne och till styrelsen eller i förekommande fall till styrelsens riskutskott.

5 § I riskchefens arbete ska det ingå att kritiskt granska och ifrågasätta beslut som påverkar företagets riskexponering. Riskchefen ska ha en löpande dialog med styrelsen och verkställande direktören om riskrelaterade frågor.

6 § Ett företag ska ha interna regler för att utse och ersätta en riskchef enligt 4 §. Styrelsen ska godkänna och besluta om tillsättning av och byte av riskchefen. Företaget ska när det tillsätter eller byter riskchef informera Finansinspektionen om detta.

8 kap. Regelefterlevnad

1 § Ett företag ska ha aktuella och lämpliga interna regler och rutiner för att kunna identifiera vilka risker som finns för att företaget inte fullgör sina förpliktelser enligt dels lagar, förordningar och andra regler som gäller för den tillståndspliktiga verksamheten, dels interna regler.

Styrelsen ska besluta om de interna reglerna för regelefterlevnad.

Företaget ska ha lämpliga rutiner och vidta lämpliga åtgärder för att minimera risken för att lagar, förordningar och andra regler som gäller för den tillståndspliktiga verksamheten inte följs.

Företaget ska när det utformar interna regler och rutiner enligt första stycket ta hänsyn till verksamhetens art, omfattning och komplexitet, och arten på och omfattningen av dess tjänster och verksamhet.

Funktion för regelefterlevnad

2 § Företagets funktion för regelefterlevnad enligt 6 kap. 1 § ska vara direkt underställd den verkställande direktören. Företaget ska utse en person som ansvarar för funktionen och för all rapportering om regelefterlevnad.

3 § Funktionen för regelefterlevnad ska

1. dels identifiera vilka risker som finns för att företaget inte fullgör sina förpliktelser enligt lagar, förordningar och andra regler som gäller för den tillståndspliktiga verksamheten, dels övervaka och kontrollera att riskerna hanteras av berörda funktioner,
2. övervaka och kontrollera efterlevnaden av dels lagar, förordningar och andra regler, dels relevanta interna regler,
3. ge råd och stöd till företagets personal, verkställande direktör och styrelse om dels de lagar, förordningar och andra regler som gäller för den tillståndspliktiga verksamheten, dels interna regler,
4. informera och utbilda berörda personer om nya eller ändrade regler,
5. kontrollera att nya, eller väsentligt förändrade, produkter, tjänster, marknader, processer, it-system samt större förändringar i företagets verksamhet och organisa-

tion följer de lagar, förordningar och andra regler som gäller för företagets tillståndspliktiga verksamhet,

6. övervaka och kontrollera att de interna reglerna och rutinerna enligt 1 § följs,

7. kontrollera och regelbundet bedöma om företagets rutiner och åtgärder enligt 1 § tredje stycket är ändamålsenliga och effektiva, och

8. lämna rekommendationer till berörda personer baserade på de iakttagelser som funktionen gjort.

9 kap. Funktion för internrevision

1 § Företagets funktion för internrevision enligt 6 kap. 1 § ska vara direkt underställd företagets styrelse.

2 § Personalen i funktionen för internrevision får inte delta i andra funktioners arbete, i den operativa verksamheten eller i arbetet med att utforma och välja riskmodeller eller andra verktyg för att hantera risk.

3 § Funktionen för internrevision ska bestå av personer med kunskap bland annat om

1. företagets verksamhet, rutiner, it-system, redovisning och värdering av tillgångar samt de risker företaget är exponerat för,

2. de lagar, förordningar och andra regler som gäller för verksamheten och

3. standarder för internrevision.

4 § Ett företag ska löpande informera och utbilda personalen i funktionen för internrevision om nya produkter och tjänster på de finansiella marknaderna.

5 § Funktionen för internrevision ska

1. arbeta efter en aktuell och riskbaserad revisionsplan som styrelsen fastställt,

2. granska och regelbundet utvärdera om företagets organisation, styrningsprocesser, it-system, modeller och rutiner är ändamålsenliga och effektiva,

3. granska och regelbundet utvärdera om företagets interna kontroll är ändamålsenlig och effektiv,

4. granska och regelbundet utvärdera om verksamheten drivs i enlighet med företagets interna regler,

5. granska och regelbundet utvärdera företagets riskhantering utifrån den beslutade riskstrategin och riskaptiten,

6. granska och utvärdera om företagets interna regler är lämpliga och förenliga med lagar, förordningar och andra regler,

7. granska och utvärdera tillförlitligheten i företagets finansiella rapportering, inklusive åtaganden utanför balansräkningen,

8. granska och regelbundet utvärdera tillförlitligheten och kvaliteten på det arbete som utförs inom företagets övriga kontrollfunktioner,

9. lämna rekommendationer till berörda personer, baserade på de iakttagelser som funktionen gjort, och

10. följa upp om åtgärderna enligt 9 genomförs. (FFFS 2014:30)

10 kap. Uppdragsavtal

1 § I detta kapitel avses med arbete och funktioner som är av väsentlig betydelse för verksamheten de tjänster som anges i 7 kap. 1 § lagen (2004:297) om bank- och finansieringsrörelse, verksamhet som har ett naturligt samband med dessa tjänster och företagets stödfunktioner.

2 § Bestämmelser om att ett institut ska anmäla till Finansinspektionen om det vill uppdra åt någon annan att utföra någon av de tjänster som avses i 7 kap. 1 § lagen (2004:297) om bank- och finansieringsrörelse och ge in uppdragsavtalet finns i 6 kap. 7 § samma lag.

Allmänna råd

Om företaget uppdrar arbete och funktioner av väsentlig betydelse för verksamheten åt någon annan, utöver det som avses i 7 kap. 1 § lagen (2004:297) om bank- och finansieringsrörelse, bör företaget anmäla detta i förväg till Finansinspektionen och lämna in uppdragsavtalet. (FFFS 2014:30)

2a § Ett företag ska ha interna regler för att hantera sina uppdragsavtal.

Styrelsen eller den verkställande direktören ska besluta om de interna reglerna. (FFFS 2014:30)

3 § Ett företag som uppdrar åt någon annan att utföra arbete och funktioner som är av väsentlig betydelse för verksamheten, ska se till att det har personal med tillräcklig kompetens och erfarenhet för att säkerställa att företaget har kontroll över den utlagda verksamheten.

4 § Ett företag som uppdrar åt någon annan att utföra arbete och funktioner som är av väsentlig betydelse för verksamheten, ska se till att uppdragstagaren i tillämpliga delar följer de regler som gäller för den tillståndspliktiga verksamheten.

5 § Ett företag ska handla med den skicklighet, omsorg och aktsamhet som krävs när det ingår, hanterar och säger upp uppdragsavtal som avser arbete eller funktioner som är av väsentlig betydelse för verksamheten.

Företaget ska säkerställa att

1. uppdragstagaren har den kompetens, kapacitet och de tillstånd som krävs enligt lag för att utföra den utlagda verksamheten tillförlitligt och professionellt,

2. uppdragstagaren utför den utlagda verksamheten effektivt och företaget ska i detta syfte fastställa metoder för att bedöma hur väl uppdragstagaren utför sina uppgifter,

3. uppdragstagaren övervakar hur den utför den utlagda verksamheten och hanterar riskerna i samband med detta på lämpligt sätt,
4. företaget vidtar lämpliga åtgärder om uppdragstagaren inte utför den utlagda verksamheten på ett effektivt sätt och enligt tillämpliga lagar och andra bestämmelser,
5. företaget dels har den kunskap som krävs för att effektivt kunna övervaka den utlagda verksamheten och hantera de risker som kan uppstå i samband med utläggandet, dels övervakar den utlagda verksamheten och hanterar dessa risker,
6. uppdragstagaren har en skyldighet att underrätta företaget om händelser som väsentligt kan påverka uppdragstagarens möjlighet att effektivt utföra den utlagda verksamheten enligt tillämpliga lagar, förordningar och andra regler,
7. företaget informerar Finansinspektionen om väsentliga förändringar i den utlagda verksamheten,
8. kontinuiteten och kvaliteten på de tjänster som företaget erbjuder sina kunder inte påverkas vid uppdragsavtalets uppsägning,
9. företaget, dess revisorer och Finansinspektionen har tillgång till uppgifter om den utlagda verksamheten samt tillträde till uppdragstagarens lokaler,
10. uppdragstagaren skyddar all konfidentiell information som avser företaget eller dess kunder, och
11. uppdragstagaren har lämpliga planer för att återställa verksamheten dels efter oförutsedda händelser, dels för återkommande test av rutinerna för backup, om det är nödvändigt med hänsyn till de delar av verksamheten som har lagts ut på uppdragstagaren. (FFFS 2014:30)

6 § Ett företag ska se till att företagets och uppdragstagarens rättigheter och skyldigheter regleras genom ett skriftligt uppdragsavtal.

7 § Om ett företag och en uppdragstagare ingår i samma konsoliderade situation enligt artikel 18 tillsynsförordningen, får företaget när det tillämpar 5, 6, 8 och 9 §§, beakta i vilken utsträckning det kontrollerar uppdragstagaren eller har möjlighet att utöva inflytande över denne. (FFFS 2014:30)

Uppdragstagare i ett land utanför EES

8 § Om ett företag uppdrar åt en uppdragstagare i ett land utanför EES att utföra en investeringstjänst i form av diskretionär portföljförvaltning för icke-professionella kunder, ska företaget, utöver att uppfylla det som anges i 5–7 §§, säkerställa att

1. den som utför uppdraget är auktoriserad eller registrerad av en tillsynsmyndighet i sitt hemland för att utföra den aktuella verksamheten och omfattas av stabilitetstillsyn, och
2. det finns ett samarbetsavtal mellan Finansinspektionen och uppdragstagarens tillsynsmyndighet.

9 § Ett företag som inte uppfyller det som anges i 8 §, får endast uppdra investeringstjänster åt en uppdragstagare i ett land utanför EES, om

1. företaget på förhand anmäler uppdragsavtalet till Finansinspektionen, och
2. Finansinspektionen inte har något att invända mot avtalet efter att ha tagit emot anmälan. (FFFS 2014:30)

Ikraftträdande- och övergångsbestämmelser

FFFS 2014:1

Dessa föreskrifter träder i kraft den 1 april 2014 utom i fråga om 2 kap. 7 § som träder i kraft den 1 januari 2015.

FFFS 2014:30

Dessa föreskrifter träder i kraft den 2 augusti 2014.

FFFS 2016:8

Dessa föreskrifter träder i kraft den 1 februari 2016.

FFFS 2017:8

Dessa föreskrifter träder i kraft den 3 januari 2018.

FFFS 2021:21

Dessa föreskrifter träder i kraft den 7 juli 2021.

FFFS 2024:28

Dessa föreskrifter träder i kraft den 17 januari 2025.