

Finansinspektionens författningssamling

Utgivare: Gent Jansson, Finansinspektionen, Box 6750, 113 85 Stockholm.
Beställningsadress: Thomson Fakta AB, Box 6430, 113 82 Stockholm. Tfn 08-587 671 00, Fax 08-587 671 71.
Prenumerera också per e-post på www.fi.se.
ISSN 1102-7460

Finansinspektionens allmänna råd om styrning och kontroll av finansiella företag;

FFFS 2005:1

Utkom från trycket
den 23 februari 2005

beslutade den 7 februari 2005.

Finansinspektionen lämnar följande allmänna råd.

1 kap. Tillämpningsområde

1 § Med dessa allmänna råd vill Finansinspektionen verka för en god styrnings- och kontrollkultur samt adekvata funktioner för styrning och kontroll i företag under myndighetens tillsyn.

2 § De allmänna råden omfattar verksamheten i företag som står under Finansinspektionens tillsyn (nedan benämnda företag) och bör tillämpas av:

– enskilda företag och, där det är lämpligt, inom koncerner, finansiella företagsgrupper, och finansiella konglomerat.

De gäller dock inte för

– företag i dess verksamhet enligt lagen (2004:46) om investeringsfonder, och
– finansiella institut enligt lagen (2004:297) om bank- och finansieringsrörelse.

3 § Finansinspektionen har även utfärdat allmänna råd om hantering av specifika riskområden inom olika företag. Dessa allmänna råd avser att komplettera dem.

Följ eller förklara

4 § De allmänna råden är generellt utformade och medger alternativa lösningar. Sådana lösningar bör kunna motiveras.

Definitioner

5 § Med *funktion* menas en eller flera personer, enheter eller avdelningar, eller särskilt tillsatta kommittéer, som fått i uppdrag att utföra en eller flera av de uppgifter som nämns i dessa allmänna råd.

Med *interna regler* avses policy- och styrdokument, riktlinjer, instruktioner eller andra skriftliga dokument genom vilka utfärdaren (styrelse, verkställande direktör eller någon annan befattningshavare) styr verksamheten.

Med *intern styrning och kontroll* menas en process genom vilken företagets styrelse, verkställande direktör, ledning och annan personal skaffar sig rimlig säkerhet för att företagets mål uppnås på följande områden:

- en ändamålsenlig och effektiv organisation och förvaltning av verksamheten
- en tillförlitlig finansiell rapportering
- efterlevnad av tillämpliga lagar, förordningar och andra regler

2 kap. Styrning

Styrelsens ansvar och uppgifter

1 § Ett företags styrelse har det yttersta ansvaret för företagets organisation och förvaltningen av dess angelägenheter. Innebörden av styrelsens ansvar följer bland annat av den associationsrättsliga och näringsrättsliga lagstiftning som företaget tillämpar.

Styrelsen bör fastställa en strategi och mål för den verksamhet som företaget driver. Styrelsen bör även följa upp att dessa mål nås.

Väsentliga förändringar som avser verksamhet och organisation bör beslutas av styrelsen.

2 § Om ett företag är moderföretag i en koncern, bör moderföretagets styrelse verka för att gemensamma interna regler fastställs för den tillståndspliktiga verksamheten som drivs av företag inom koncernen. Detsamma bör gälla för det företag i en finansiell företagsgrupp eller ett finansiellt konglomerat som har en överordnad ställning inom gruppen eller konglomeratet.

Om det är lämpligt kan de funktioner som behandlas i 4 kap. (Riskhantering och riskkontroll), 5 kap. (Regelefterlevnad) och 6 kap. (Oberoende granskningsfunktion), placeras centralt inom en koncern, en finansiell företagsgrupp eller ett finansiellt konglomerat. Detta gäller under förutsättning att funktionerna har kompetens och resurser som avser samtliga tillståndspliktiga verksamheter.

3 § Även i företag som inte omfattas av aktiebolagslagen bör styrelsen i interna regler fastställa en arbetsordning för styrelsen samt uppgifterna för verkställande direktören eller motsvarande befattningshavare.

Verkställande direktörens ansvar och uppgifter

4 § Ett företags verkställande direktör sköter den löpande förvaltningen av företagets angelägenheter enligt styrelsens riktlinjer och anvisningar. Verkställande direktören vidtar även de åtgärder som krävs för att

- företagets bokföring fullgörs i enlighet med lag, och att
- medelsförvaltningen sköts på ett betryggande sätt.

Innebörden av den verkställande direktörens ansvar följer bland annat av den associationsrättsliga och näringsrättsliga lagstiftningen.

Verkställande direktören bör se till att styrelsen dels får sådan saklig, utförlig och relevant information som behövs för att den ska kunna fatta väl underbyggda beslut, dels att styrelsen löpande informeras om utvecklingen av företagets verksamhet.

Intern information

5 § Ett företag bör ha effektiva informations- och kommunikationssystem för intern information. Här avses bland annat tekniska system samt organisation och rutiner för kommunikation och spridning av information internt.

3 kap. Intern styrning och kontroll

1 § Genom en god intern kontroll kan ett företag säkerställa

- en ändamålsenlig och effektiv organisation och förvaltning av verksamheten,
- en tillförlitlig finansiell rapportering,
- en effektiv drift och förvaltning av informationssystem,
- en god förmåga att identifiera, mäta, övervaka och hantera sina risker,
- en god förmåga att efterleva lagar och förordningar, interna regler, samt god sed eller god standard.

2 § Styrelsen och verkställande direktören bör verka för att en god intern kontroll präglar organisationen och driften av företagets verksamhet.

3 § För att upprätthålla en god intern kontroll bör organisationen anpassas till de förändringar i interna och externa risker som inträffar över tiden.

4 § Ett företag kan uppnå en god intern kontroll genom att exempelvis:

- följa upp verksamheten löpande och se till att det finns kontroller som säkerställer att rapporteringen på ett rimligt sätt återspeglar verksamheten,
- kontrollera löpande att resurser utnyttjas effektivt och i syfte att nå företagets mål,
- ta fram interna regler, samt dokumentera och uppdatera dessa löpande,
- fördela ansvar och arbete så att risken för intressekonflikter undviks,
- se till att en befattningshavare inte ensam handlägger en transaktion genom hela behandlingskedjan (dualitetsprincipen),
- säkerställa genom kontroller att information lämnas om utvecklingen inom ett verksamhetsområde avviker från riktlinjer och mål i företaget,
- säkerställa genom kontroller att redovisningen är fullständig och riktig, transaktioner rapporteras i tid samt att redovisade transaktioner verkligen är genomförda,
- säkerställa genom kontroller för informationssäkerhet och fysisk säkerhet, kontinuitet i verksamheten och skydda företagets och kundernas tillgångar,
- se till att informations- och rapporteringssystem säkerställer aktuell och relevant information om institutets verksamhet och riskexponering etc.

4 kap. Hantering och kontroll av risker

Risker i verksamheten

1 § Risker som bör hanteras och kontrolleras är exempelvis följande:

- kredit- och motpartsrisker,
- marknadsrisker (ränte-, valuta- och kursrisker),
- likviditetsrisker,
- operativa risker (risken för förluster till följd av att interna processer och rutiner är felaktiga eller inte ändamålsenliga, mänskliga fel, felaktiga system eller externa händelser inklusive legala risker).

För försäkringsbolag och understödsföreningar finns därutöver specifika försäkringsrisker, så som

- teckningsrisker,
- reservsättningsrisker,
- återförsäkringsrisker, och
- matchningsrisker.

Interna regler för hantering och kontroll av risker

2 § Styrelsen bör se till att företagets hantering av risker (riskhantering) och uppföljningen av företagets risker (riskkontroll) är tillfredsställande.

För detta ändamål bör det fastställas interna regler i fråga om riskhanteringen och riskkontrollen. Det bör löpande säkerställas att dessa regler följs.

Hur ska riskkontrollen organiseras?

3 § Det bör finnas en samlad funktion i företaget för självständig riskkontroll. Funktionen bör informera styrelse, ledning och i övrigt dem som har behov av informationen.

Informationen bör ge en allsidig och saklig bild av företagets risker samt innehålla analyser av utvecklingen av riskerna. Funktionen bör också föreslå de ändringar i styrdokument och processer som funktionens iakttagelser om riskhanteringen ger anledning till.

Funktionen bör vara underställd den verkställande direktören. Den kan även vara placerad under en annan ledande befattningshavare med goda kunskaper om företagets risker, som är direkt underställd den verkställande direktören. Denna person ska dock inte ha ansvar för den dagliga affärsverksamheten .

Funktionen bör ha tillräckliga resurser för sina uppgifter. Uppgifterna bör inte utföras av befattningshavare som arbetar med den dagliga affärsverksamheten.

4 § Funktionen kan utforma arbetet på olika sätt beroende på företagets verksamhet. Den kan t.ex. uppdra åt andra funktioner i företaget att sammanställa underlag för dess rapporter och analyser. Funktionen ansvarar dock alltid för den samlade rapporteringen och analysen av företagets risker liksom för att underliggande data är korrekta.

5 § För försäkringsbolag gäller dessutom 8 kap. 1 § och 16 kap. 1 § försäkringsrörelselagen (1982:713) om den ansvarige aktuariens uppgifter och ansvar.

5 kap. Regelefterlevnad (Compliance)

1 § Med *regelefterlevnad* menas i dessa allmänna råd efterlevnad av lagar, förordningar och interna regler samt god sed eller god standard (nedan gemensamt benämnda regler) avseende den tillståndspliktiga verksamheten.

Bristande regelefterlevnad kan leda till ökade operativa risker, risker för juridiska sanktioner, tillsynssanktioner, ekonomiska förluster eller ryktesförluster.

Hur ska regelefterlevnaden säkerställas?

2 § Styrelsen bör se till att det finns en funktion (compliance) som utgör ett stöd för att verksamheten drivs enligt gällande regler. Funktionen bör också, om det är lämpligt, följa upp regelefterlevnaden.

Funktionen bör löpande informera om de risker som kan uppkomma i verksamheten till följd av bristande regelefterlevnad, hjälpa till med att identifiera och bedöma sådana risker samt biträda vid utformningen av interna regler. Funktionen bör också informera styrelsen, verkställande direktören och ledningen i frågor om regelefterlevnad.

3 § Funktionen bör löpande se till att den personal som berörs får information om nya eller ändrade regler och, om det behövs, utbildning i nya regelverk.

4 § Styrelsen eller verkställande direktören bör utfärda interna regler för funktionens ansvarsområde, omfattningen och genomförandet av funktionens arbete samt rutiner för information om iakttagelser.

5 § Funktionen bör vara underställd styrelsen, eller den verkställande direktören. Den kan även vara placerad under en annan ledande befattningshavare med goda kunskaper om företagets risker och verksamheten i övrigt, som är direkt underställd den verkställande direktören.

Funktionen bör ha tillräckliga resurser för sina uppgifter. Den bör även ha personal med goda kunskaper om företagets risker och de regler som företaget tillämpar.

6 § Funktionens arbete kan utformas på olika sätt beroende på företagets verksamhet. Det kan variera dels mellan olika företag, dels inom ett företag exempelvis på lokal och central nivå.

Strävan bör vara att funktionen så långt det är möjligt når en självständig ställning i förhållande till den direkt affärsdrivande verksamheten. Funktionens arbete kan om det är lämpligt utföras av konsulter.

7 § För värdepappersföretag gäller dessutom 3 kap. Finansinspektionens föreskrifter (FFFS 2002:7) om uppföranderegler på värdepappersmarknaden.

6 kap. Oberoende granskningsfunktion (Internrevision)

1 § Styrelsen bör se till att det finns en funktion som granskar och utvärderar den interna kontrollen (som innefattar riskkontrollen och compliancefunktionen). I de företag som har en funktion för internrevision bör det vara denna som utför uppgifterna.

Funktionen bör ha tillräckliga resurser för sina uppgifter. Den bör även ha personal med

– goda kunskaper om företagets risker och de regler som företaget tillämpar, samt
– särskild kompetens för att granska och utvärdera utveckling, drift och förvaltning av företagets informationssystem.

2 § Funktionen bör vara direkt underställd styrelsen. Organisatoriskt bör den vara helt separerad från verksamheten som ska granskas. Funktionens oberoende innebär alltså att den inte bör delta i den operativa verksamheten.

3 § Styrelsen bör i interna regler fastställa funktionens ansvar, arbetsuppgifter, och rutiner för rapportering.

4 § Funktionen bör följa upp att verksamhetens omfattning och inriktning överensstämmer med styrelsens interna regler. Funktionen bör också granska och utvärdera företagets organisation och rutiner. Chefen för funktionen bör närvara vid de styrelsesammanträden då funktionens rapporter behandlas.

5 § Granskningen kan, om det är lämpligt, utföras av konsulter.

6 § Funktionens arbete bör dokumenteras.

7 kap. Uppdragsavtal

1 § Ett företag kan lägga ut delar av verksamheten till en uppdragstagare utanför företaget, såväl inom som utom den egna koncernen eller företagsgruppen. Styrelsen och verkställande direktören ansvarar dock alltid för den verksamhet som lagts ut.

2 § Styrelsen eller verkställande direktören bör upprätta interna regler om vilka tillståndspliktiga verksamheter, eller verksamheter som har ett naturligt samband med finansiell verksamhet eller dess stödfunktioner, som kan läggas ut och hur detta ska göras.

Av de interna reglerna bör åtminstone följande framgå:

- vilka krav som ska ställas på företagets beställarkompetens,
- hur risker med utläggningen ska hanteras,
- att företaget ska försäkra sig om att uppdragstagaren skyddar konfidentiell information både när det gäller företaget och dess kunder,
- hur företaget ska styra och följa upp hur uppdraget utförs samt revidera den utlagda verksamheten,
- vilka krav som dels ska ställas på kompetens hos uppdragstagaren, dels på intern kontroll och kvalitet, samt uppdragstagarens möjligheter att långsiktigt fullgöra sitt uppdrag,
- att företaget och uppdragstagaren ska upprätta och vidmakthålla beredningsplaner för oförutsedda händelser, inklusive en kris- och katastrofplanering som löpande ska testas,

- att det ska säkerställas att Finansinspektionen fortsättningsvis kan driva en effektiv tillsyn över företaget, liksom att företagets skyldigheter mot Finansinspektionen eller företagets kunder inte åsidosätts,
- att det ska upprättas beredskapsplaner och strategier för hur uppdraget ska kunna avslutas och verksamheten återtas till företaget, utan betydande störningar av viktig verksamhet,
- att det ska upprättas ett skriftligt avtal, som reglerar servicenivå, parternas rättigheter och skyldigheter samt övriga frågor enligt dessa allmänna råd.

3 § Vid utläggning av verksamhet inom en koncern eller en företagsgrupp bör frågor om jäv och intressekonflikter särskilt uppmärksammas. Styrelsen bör se till att samtliga dessa frågor identifieras och att företaget har interna regler som hanterar frågor om jäv och intressekonflikter.

4 § Om ett företag avser att lägga ut en betydande del av den tillståndspliktiga verksamheten, eller verksamhet som har ett naturligt samband med finansiell verksamhet eller dess stödfunktioner, bör företaget anmäla detta i förväg till Finansinspektionen.

5 § För banker och kreditmarknadsföretag gäller dessutom 6 kap. 7 § lagen (2004:297) om bank- och finansieringsrörelse.

För försäkringsbolag gäller även 8 kap. 8 § försäkringsrörelselagen (1982:713).

För värdepappersföretag gäller dessutom Finansinspektionens allmänna råd (FFFS 2002:5) om värdepappersrörelse.

Dessa allmänna råd träder i kraft den 1 maj 2005, då följande författningar ska upphöra att gälla:

1. Finansinspektionens allmänna råd (FFFS 1999:12) om styrning, intern information och intern kontroll inom kredit- och värdepappersinstitut samt i fondbolag,
2. Finansinspektionens allmänna råd (FFFS 2000:3) om styrning, intern information och intern kontroll inom försäkringsbolag och understödsföreningar.

INGRID BONDE

Hans Schedin