

Till kreditinstitutens holdingsammanslutningar

Till kreditinstituten

FÖRESKRIFT OM RISKHANTERING OCH ÖVRIG INTERN KONTROLL I KREDITINSTITUT

Finansinspektionen meddelar med stöd av 68 § 2 mom. kreditinstitutslagen (1607/1993) följande föreskrift om riskhantering och övrig intern kontroll i ett kreditinstitut och i företag som hör till dess konsolideringsgrupp.

Föreskriften beaktar rådets andra direktiv 89/646/EEG av den 15 december 1989 om samordning av lagar och andra författningar om rätten att starta och driva verksamhet i kreditinstitut, samt med ändring av direktiv 77/780/EEG (EGT nr L 386, 30.12.1989, s.1) och rådets direktiv 93/22/EEG av den 10 maj 1993 om investeringstjänster inom värdepappersområdet (EGT nr L 141, 19.6.1993, s. 27).

Föreskriftens syfte och tillämpningsområde

I denna föreskrift fastställer Finansinspektionen minimikraven för adekvat riskhantering och övrig intern kontroll. Utgångspunkten är att riskhanteringen och den övriga interna kontrollen i ett kreditinstitut och i företag som hör till dess konsolideringsgrupp är av tillräckligt hög standard med hänsyn till verksamhetens karaktär och omfattning, att kreditinstitutet eller ett företag i samma konsolideringsgrupp inte tar för stora risker i sin verksamhet och att kontrollrutinerna är av den arten att sådana risker i affärsverksamheten kan upptäckas, analyseras och begränsas. Om principerna för riskhantering och övrig intern kontroll meddelar Finansinspektionen anvisning 108.2. I anvisningen ger Finansinspektionen rekommendationer för rutinerna för sådan riskhantering och övrig intern kontroll som denna föreskrift kräver. Vad som i denna föreskrift sägs om kreditinstitut tillämpas också på kreditinstitutets holdingsammanslutning och på andra företag i samma konsolideringsgrupp.

Definition av begreppet intern kontroll

Den interna kontrollen är en process som syftar till att säkerställa

- a) måluppfyllelse
- b) ekonomiskt och effektivt utnyttjande av resurser
- c) adekvat kontroll av riskerna i verksamheten
- d) tillförlitlig och riktig ekonomisk och övrig information för ledningen
- e) efterlevnad av lagar och föreskrifter samt strategier, planer, interna regler och rutiner.

Enligt definitionen omfattar den interna kontrollen all ekonomisk och övrig kontroll som utförs av direktionen/styrelsen, det förvaltningsorgan som övervakar direktionens/styrelsens verksamhet, den verkställande ledningen och övrig personal.

Med den interna kontrollen integrerad riskhantering

Med riskhantering avses identifiering, analys, begränsning och kontroll av de risker som affärsverksamheten medför och som väsentligen hör till affärsverksamheten¹. Riskhanteringen i kreditinstitut är integrerad med den interna kontrollen.

Det väsentliga i riskhanteringen är att identifiera riskerna i företagets olika funktioner och att fastställa verksamhetsprinciper för begränsning av riskerna.

Riskhanteringsrutinerna kan avvika mellan olika institut beroende på affärsverksamhetens omfattning och karaktär.

De viktigaste elementen i den interna kontrollen är

- a) ledarskaps- och kontrollkultur
- b) identifiering, analys, begränsning och kontroll av riskerna
- c) kontrollåtgärder och åtskiljande av uppgifterna

- d) rapportering och informationsförmedling
- e) övervakning av funktionerna och avhjälpande av brister.

Ansaret för riskhanteringen och den övriga interna kontrollen

Kreditinstitutets ledning har det primära ansvaret för att intern kontroll införs. Beroende på institutets storlek, omfattningen av verksamheten och den juridiska organisationsformen (aktiebolag, affärsbank, sparbank, andelsbank eller förening) finns avsevärda skillnader i fråga om förvaltningsorganen och ansvarsfördelningen mellan dem. I föreskriften specificeras därför inte uppgifterna för t.ex. direktionen och förvaltningsrådet i en affärsbank, utan arbetsfördelningen bestäms av speciallagarna och den lagbundna praxisen. Ledningsansvaret för olika delområden bestäms av lagstiftning, interna föreskrifter och instruktioner samt av kreditinstitutets storlek.

¹ Mätning och begränsning av riskerna med hjälp av limiter gäller endast risker som kan mätas på förhand.

Det kreditinstitut eller den holdingsammanslutning som är moderföretag i konsolideringsgruppen svarar för att strategier och verksamhetsprinciper för riskhanteringen och den övriga interna kontrollen i konsolideringsgruppen fastställs. Förvaltningsorganet med högsta beslutanderätt i moderföretaget skall på ett övergripande sätt övervaka att principerna för den interna kontrollen följs av de organisationer i vilka det har ägarkontroll. Det högsta förvaltningsorganets ansvar befriar likväl inte t.ex. styrelsen/direktionen för ett kreditinstitut som är dotterföretag i koncernen från ansvaret att införa intern kontroll i sin egen organisation.

Allmänna principer för intern kontroll

Följande principer är gemensamma för alla delområden av den interna kontrollen:

- a) Den interna kontrollen skall främja en företagskultur som ser den interna kontrollen som en naturlig och nödvändig del av företagsverksamheten.
- b) Den interna kontrollen skall täcka alla funktioner i kreditinstitutet. Kontrollen skall dimensioneras i rätt proportion till riskerna i de olika verksamheterna. Särskild vikt skall fästas vid nya produkter och verksamheter samt internationella engagemang.
- c) Moderföretaget i kreditinstitutets konsolideringsgrupp skall se till att företagen i dess konsolideringsgrupp har en adekvat intern kontroll.
- d) Den interna kontrollen skall också täcka tjänster som köps från andra företag.
- e) Den interna kontrollen skall omfatta ett sådant riskhanteringssystem att alla större risker i ett kreditinstituts verksamhet kan identifieras, analyseras och kontrolleras.
- f) Den interna kontrollen skall förhindra bedrägeri, försnillning och andra oegentligheter.
- g) Kreditinstitutet skall se till att det finns uppdaterade instruktioner för centrala verksamhetsområden, inklusive intern kontroll.
- h) Intern kontroll innebär också beredskap för störningar i verksamheten. Kreditinstitutet skall ha utarbetat planer som säkerställer kontinuitet i verksamheten, och planerna skall testas för att kontrollera att de fungerar.
- i) Kreditinstitutets direktion eller styrelse intar en central roll när det gäller att fastställa riskhanteringsprinciperna och –rutinerna och genomföra kontrollen, oavsett vilket förvaltningsorganens ansvar är enligt lag eller interna föreskrifter och instruktioner.

Kreditinstitutet skall fästa särskild uppmärksamhet vid följande detaljer i fråga om varje element i den interna kontrollen:

Ledarskaps- och kontrollkultur

Kreditinstitutet skall

- 1) bestämma kreditinstitutets affärsstrategier, verksamhetsprinciper och organisationsstruktur samt se till att ansvar, rapporteringsförhållanden och befogenheter fördelas på ett ändamålsenligt sätt och att riskhanteringen och den övriga interna kontrollen täcker institutets samtliga funktioner och är rätt dimensionerade i förhållande till riskerna i de olika verksamheterna
- 2) fastställa kvantitativa och kvalitativa mål för varje delområde av kreditinstitutets verksamhet samt kontrollera att målen uppfylls
- 3) säkerställa att personalen är kompetent och lämpad för sina arbetsuppgifter och har den information som behövs för att uppgifterna skall kunna utföras.

Identifiering, analys, begränsning och kontroll av riskerna

Kreditinstitutet skall

- 4) försäkra sig om att riskerna i affärsverksamheten identifieras och analyseras
- 5) fastställa principer för riskexponeringen samt slå fast rutiner för riskbegränsningen och övervaka att de följs
- 6) försäkra sig om att kreditinstitutet har en riskkontrollfunktion som är oberoende av risktagningsfunktionen.

Kontrollåtgärder och åtskiljande av uppgifterna

Kreditinstitutet skall

- 7) säkerställa att de interna kontrollrutinerna integreras med kreditinstitutets dagliga rutiner och att farliga arbetskombinationer har delats upp på flera anställda och rutinerna för de viktigaste funktionerna har skriftligen dokumenterats
- 8) säkerställa att anställda som representanter för kreditinstitutet inte handlägger affärstransaktioner som berör dem själva eller personer i deras närmaste krets eller på annat sätt deltar i beslut om sådana transaktioner.

Rapportering och informationsförmedling

Kreditinstitutet skall

- 9) säkerställa att kreditinstitutet har adekvata rapporterings- och informationssystem till stöd för beslutsfattandet och utvärderingen av verksamheten

-
- 10) säkerställa att kreditinstitutet har adekvata och ändamålsenliga datasystem.

Övervakning av funktionerna och avhjälpande av brister

Kreditinstitutet skall

- 11) säkerställa att internrevisionen är organiserad på ett ändamålsenligt sätt och att den fungerar enligt god intern revisionsssed
- 12) säkerställa att direktionen eller styrelsen och de förvaltningsorgan som övervakar direktionens eller styrelsens verksamhet delges alla viktiga observationer som görs av interna och externa revisorer och av myndigheter
- 13) se över den interna kontrollen och riskhanteringen regelbundet och alltid när
- kreditinstitutet inleder verksamhet på en ny marknad
 - kreditinstitutet introducerar en ny produkt
 - omvärlden har förändrats eller kommer att förändras väsentligt eller
 - affärsverksamheten omorganiseras
- 14) utarbeta rutiner för att säkerställa att den interna kontrollen ses över om den visar sig vara bristfällig.

Närmare upplysningar lämnas av: Kreditinstitutsavdelningen