

Till fondbörserna

Anvisning om riskhantering och övrig intern kontroll i fondbörser

Finansinspektionen meddelar med stöd av 4 § 2 punkten lagen om finansinspektionen följande anvisning om principerna för riskhantering och intern kontroll och om internrevision i fondbörser.

INNEHÅLL

	Sida
1 Inledning	3
2 Definition av processen för intern kontroll och riskhantering	4
2.1 Intern kontroll	4
2.2 Riskhantering	4
3 Ansvar för den interna kontrollen och riskhanteringen	4
4 Allmänna principer för intern kontroll	6
5 Riskhanteringsprinciper	7
6 Organisationsprinciper	7
7 Principer för redovisnings- och informationssystem	8
8 Principer för datasystem	8
9 Internrevision	9
9.1 Internrevisionens roll	9
9.2 Internrevisionens ställning	10

1 Inledning

En störningsfri verksamhet på fondbörserna är av yttersta vikt för marknadens funktionsduglighet och stabilitet. Finansinspektionen har därför ansett det nödvändigt att meddela fondbörserna en anvisning om principerna för riskhantering och intern kontroll och om internrevision.

I denna anvisning fastställer Finansinspektionen minimikraven för adekvat riskhantering och övrig intern kontroll. Utgångspunkten är att riskhanteringen och den övriga interna kontrollen i en fondbörs är av tillräckligt hög standard med hänsyn till verksamhetens karaktär och omfattning. Fondbörsens kontrollrutiner skall vara av den arten att riskerna i affärsverksamheten kan upptäckas, analyseras och begränsas. En adekvat riskhantering och övrig intern kontroll skall täcka all affärsverksamhet som bedrivs av en fondbörs som beviljats koncession. Principerna i anvisningen är allmänt vedertagna och ger uttryck för ett synsätt som är gemensamt för de olika finansinspektionerna i Europa.

I anvisningens andra avsnitt definieras begreppen intern kontroll och riskhantering. Definitionerna beskriver målen för båda processerna men fastställer inte närmare hur processerna skall organiseras. Följande avsnitt behandlar ansvaret för riskhanteringen och den interna kontrollen och fastställer minimikraven på ansvaret för dessa processer.

I avsnitt fyra och fem beskrivs de allmänna principerna för intern kontroll och riskhantering och i avsnitt sex sådana omständigheter avseende riskhanteringen och den interna kontrollen som skall beaktas vid utformningen av organisationen i en fondbörs. De två följande avsnitten presenterar närmare sådana detaljer i samband med data-, redovisnings- och informationssystemen som har särskild betydelse för den interna kontrollen och riskhanteringen. Det sista avsnittet tar upp internrevisionens roll och ställning inom organisationen.

2 Definition av processen för intern kontroll och riskhantering

2.1 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 styrelsen, verkställande direktören och övrig personal.

2.2 Riskhantering

Med riskhantering avses en process som syftar till identifiering, mätning, begränsning och kontroll av de risker som affärsverksamheten medför och som väsentligen hör till affärsverksamheten¹. Riskhanteringen i fondbörsen är integrerad med den interna kontrollen.

En adekvat riskhantering skall täcka (men inte vara begränsad till) åtminstone följande riskområden:

- kreditrisk (inkl. motpartsrisk)
- finansieringsrisk
- operativ risk
- legal risk
- strategisk risk.

En adekvat riskhantering skall täcka (men inte vara begränsad till) de riskområden som är väsentliga med tanke på kontinuiteten i fondbörsens kärnverksamhet.

3 Ansvaret för den interna kontrollen och riskhanteringen

Fondbörsens styrelse intar en central roll när det gäller att fastställa och övervaka principerna och rutinerna för den interna kontrollen.

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

Fondbörsens styrelse fastställer principerna för risktagning och sörjer för att fondbörsen har ett riskhanterings- och kontrollsystem som är rätt dimensionerat i proportion till verksamhetens omfattning och karaktär. Fondbörsens styrelse och verkställande direktör ansvarar för att den interna kontrollen ingår som en väsentlig del i alla verksamheter.

Om fondbörsen ingår i en koncern kan en del av den interna kontrollen och riskhanteringen på grund av intern arbetsfördelning höra till styrelsen och verkställande direktören i koncernens moderbolag. Fondbörsens styrelse och verkställande direktör ansvarar dock alltid i första hand för att fondbörsens riskhantering och interna kontroll är effektiv och adekvat.

Fondbörsens styrelse och verkställande direktör skall särskilt

- 1) bestämma fondbörsens organisationsstruktur samt se till att ansvar och befogenheter fördelas på ett ändamålsenligt sätt och att den interna kontrollen och riskhanteringen täcker fondbörsens samtliga funktioner och är rätt dimensionerade i förhållande till riskerna i de olika verksamheterna
- 2) fastställa kvantitativa och kvalitativa mål för varje delområde av fondbörsens verksamhet samt kontrollera att målen uppfylls
- 3) fastställa principer för riskexponeringen samt slå fast rutiner för riskbegränsningen och övervaka att de följs
- 4) säkerställa att personalen är kompetent och lämpad för sina arbetsuppgifter och har den information som behövs för att uppgifterna skall kunna utföras
- 5) försäkra sig om att fondbörsens viktigaste funktioner har skriftligen dokumenterats
- 6) säkerställa att fondbörsen har adekvata redovisnings- och informationssystem till stöd för beslutsfattandet och utvärderingen av verksamheten
- 7) säkerställa att kreditinstitutet har adekvata och ändamålsenliga datasystem
- 8) säkerställa att anställda som representanter för fondbörsen inte handlägger affärstransaktioner som berör dem själva eller personer i deras närmaste krets eller på annat sätt deltar i beslut om sådana transaktioner
- 9) säkerställa att internrevisionen är organiserad på ett ändamålsenligt sätt och att den fungerar enligt god intern revisionssed
- 10) säkerställa att styrelsen delges alla viktiga observationer som görs av interna och externa revisorer och av myndigheter

-
- 11) säkerställa att den interna kontrollen är organiserad så att den stöder uppfyllandet av riskhanteringsmålen
 - 12) försäkra sig om att riskkontrollfunktionen är oberoende av risktagningsfunktionen.
 - 13) se över den interna kontrollen och riskhanteringen regelbundet och alltid när
 - fondbörsen inleder verksamhet på en ny marknad
 - fondbörsen 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.

4 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 fondbörsen. 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) Fondbörsen skall se till att företagen i dess koncern har en adekvat intern kontroll.
- d) Den interna kontrollen skall också täcka tjänster som köps från andra företag eller om fondbörsen är en del av en koncern från enheter underställda koncernledningen.
- e) Den interna kontrollen skall omfatta sådana system för analys och hantering av risker att alla större risker i en fondbörs verksamhet kan identifieras, analyseras och kontrolleras.
- f) Den interna kontrollen skall förhindra bedrägeri, försnillning och andra oegentligheter. Till den interna kontrollen för att förhindra andra oegentligheter hör bl.a. kontrollen av personalens värdepappersavslut för egen räkning och av att reglerna för dessa efterlevs.
- g) Fondbörsen skall se till att det finns uppdaterade instruktioner för centrala verksamhetsområden, inklusive intern kontroll.

-
- h) Intern kontroll innebär också beredskap för störningar i verksamheten. Fondbörsen skall ha utarbetat planer som säkerställer kontinuitet i verksamheten, och planerna skall testas för att kontrollera att de fungerar.

5 Riskhanteringsprinciper

Några centrala principer för riskhanteringen:

- a) För kvantifierbara risker skall fastställas skriftliga limiter och för kvalitetsrisker skall utarbetas skriftliga rutiner.
- b) Riskhanteringen skall innefatta en beslutsordning för nya engagemang. Alla involverade bör i fråga om sina egna ansvarsområden vara medvetna om riskerna och riskhanteringen i den nya verksamheten.
- c) Efterlevnaden av limiter och rutiner skall fortlöpande kontrolleras. Limitöverskridningar och avvikelser från rutinerna skall genast utvärderas och rapporteras. För avvikelsekontrollen skall tydliga rutiner utarbetas.
- d) Limiterna och rutinerna i riskhanteringen skall regelbundet ses över så att de överensstämmer med de fastslagna riktlinjerna och det rådande marknadsläget.

6 Organisationsprinciper

Fondbörsen skall ha en organisation som är avpassad efter den verksamhet som bedrivs och de risker som förekommer i verksamheten. Organisationen skall utformas enligt följande principer:

- a) Arbetsfördelningen inom organisationen skall vara klart definierad för att underlätta kontrollen och förhindra oegentligheter och fel.
- b) Organisationen skall ha ett adekvat ersättersystem, och ledningen skall säkerställa att ersättarna också behärskar de arbetsuppgifter som de är utsedda att som ersättare sköta.
- c) För varje verksamhetsprocess skall finnas egna kontrollrutiner som säkerställer att alla åtgärder är regelrätt auktoriserade, utförda och redovisade.
- d) Tillgången till medel och konfidentiell information skall begränsas till behörig personal enligt vars och ens befattningsbeskrivning och ansvarsområde.

7 Principer för redovisnings- och informationssystem

Redovisnings- och informationssystemen säkerställer att affärstransaktionerna bokförs och informationen om dem förmedlas till interna besluts- och kontrollorgan och externa intressenter. Informationen skall ge en rättvisande bild av fondbörsens verksamhet. För att säkerställa effektiva redovisnings- och informationssystem skall följande principer följas:

- a) Varje affärstransaktion redovisas fullständigt och riktigt, i rätt tid, tillräckligt specificerat och snarast möjligt. Verifieringskedjan skall vara obruten ända från det ursprungliga dokumentet.
- b) Ledningen och övrig personal får snabbt den information de behöver för att kunna sköta sina arbetsuppgifter.
- c) Myndigheterna får sina rapporter snarast möjligt inom utsatt tid.
- d) Den externa informationen (bokslut, rapporter till tillsynsmyndigheter osv.) är upprättad enligt lagar och föreskrifter.

8 Principer för datasystem

Fondbörserna skall ha den kompetens, organisation och interna kontroll som behövs för att lagra och hantera data i elektronisk form. För den interna kontrollen innebär det att principerna under punkterna a–k nedan skall följas. De skall följas också i de fall databehandlingen har decentraliserats till affärsenheter utanför IT-avdelningen eller motsvarande enhet. Fondbörserna skall se till att de företag som anlitas för datatjänster tillämpar liknande principer.

Fondbörserna behöver i sin egen verksamhet följa principerna under punkterna a–k nedan endast i den utsträckning de själv har ifrågavarande verksamhet.

- a) Styrelsen skall anta en IT-strategi och -budget för att säkerställa att en lämplig IT-miljö existerar och underhålls enligt nuvarande och framtida behov.
- b) För informationsteknikens olika delområden definieras riktlinjer, standarder, rutiner och kontroller som möjliggör samarbete mellan affärs- och IT-enheterna. Utifrån riktlinjerna, standarderna, rutinerna och kontrollerna skall ledningen sedan planera, övervaka och utvärdera IT-funktionerna.
- c) IT-funktionens oberoende ställning i förhållande till användarna skall säkerställas. IT-funktionen ansvarar för datasystemens utveckling och funktionsförmåga, medan användarna svarar för att behandlade data är riktiga.

-
- d) Systemutveckling och datadrift separeras så att de anställda i dessa funktioner får tillgång till varandras data endast via kontrollerade standardrutiner. Också arbetsuppgifterna för personal som ansvarar för drift, underhåll, användarbehörigheter och databaser bör hållas isär.
- e) Internrevisionen skall garanteras kompetens att utvärdera de interna IT-kontrollerna vad gäller ändamålsenlighet och funktionsförmåga.
- f) Metoder för systemering och kvalitetskontroll skall utarbetas för att säkerställa att systemen fungerar på planerat sätt och att de dokumenteras i sådan standardiserad form att de går att använda och vidareutveckla i framtiden.
- g) Rutiner för inköp eller godkännande av program- och maskinvara eller för kontraktering till externa tjänsteproducenter skall utarbetas för att säkerställa att nyanskaffningar och avtal motsvarar fondbörsens behov och gällande standarder samt garanterar fortlöpande service.
- h) Kontrollmekanismer och revisionsspårning skall byggas in i datasystemen för att säkerställa indatas och resultatens riktighet och integritet, behörigheter, återställande av information efter avbrott i databehandlingen samt transaktionernas reviderbarhet.
- i) Ledningen skall fastställa enhetliga principer för beviljning av behörighet att använda data och program och för kontroll av användningen. Tillgången till data och program begränsas till behöriga användare med tekniska metoder (användaridentifikation, lösenord etc.) och överträdelser rapporteras och utreds.
- j) Med olika rutiner och riktlinjer för den fysiska säkerheten minimeras risken för avbrott i datasystemen (eldsvåda, översvämning, elavbrott etc.) och tillgången till känsligt material (datautrustning, datamedium, dokument osv.) begränsas till behörig personal.
- k) En plan för att säkerställa kontinuitet i livsviktiga funktioner skall tas fram. Vid oväntade avbrott skall en återgång till normal verksamhet vara möjlig inom en rimlig tid. Kontinuitetsplanen skall uppdateras och testas regelbundet.

9 Internrevision

9.1 Internrevisionens roll

Den interna revisionen är i regel en sakkunnigorganisation som är underställd bolagets eller koncernens moderbolags verkställande direktör och har som uppgift att analysera verksamhetsprocesserna och utifrån utförd granskning ge rekommendationer och utlåtanden. Fondbörsens betydelse för värdepappersmarknadens tillförlitlighet och effektivitet kräver att fondbörsen har en

fungerande internrevision. Om den interna revisionen är underställd verkställande direktören för koncernens moderbolag skall fondbörsens verkställande direktör och styrelse sörja för att internrevisionen är tillräcklig för att utföra de uppgifter och nå de mål som anges i anvisningen.

Fondbörsens styrelse skall fastställa arbetsuppgifterna, befogenheterna och ansvaret för den interna revisionen samt de allmänna principerna för revisionsplaneringen och rapporteringen av gjorda iakttagelser.

Följande mål och uppgifter anses i regel höra till internrevisionen:

- a) Regelbunden utvärdering av den interna kontrollen vad gäller omfattning, dimensionering i proportion till verksamheten, effektivitet och kostnader samt kontroll att riktlinjer och instruktioner som fastställts av ledningen följs.
- b) Kontroll och utvärdering av riskhanteringssystemens funktionsförmåga.
- c) Utvärdering av tillförlitligheten och integriteten av redovisnings- och datasystem och andra system som används till att mäta, kategorisera och rapportera ekonomisk och operativ information.
- d) Testning för att verifiera affärstransaktioner och den interna kontrollens funktionsförmåga.

Ledningen skall se till att dessa för den interna kontrollen så viktiga uppgifter blir utförda.

9.2 Internrevisionens ställning

Följande allmänna principer gäller för den interna revisionsfunktionen:

- a) Den skall vara oberoende i förhållande till den granskade verksamheten.
- b) Dess verksamhetsområde skall vara obegränsat för att säkerställa att alla funktioner i fondbörsen omfattas av granskningen.
- c) Den skall vara rätt dimensionerad i förhållande till fondbörsens verksamhet och ha den kompetens och erfarenhet som behövs.
- d) Den skall ha en ställning i organisationen som säkerställer att granskningsrapporterna och rekommendationerna behandlas på ett behörigt sätt i styrelsen.