

Till värdepappersföretagen

ANVISNING OM PRINCIPER FÖR RISKHANTERING OCH INTERN KONTROLL OCH OM INTERNREVISION I VÄRDEPAPPERSFÖRETAG

Finansinspektionen meddelar med stöd av 4 § 2 punkten lagen om finansinspektionen följande anvisning om principerna för riskhantering och intern kontroll och om internrevision i ett värdepappersföretag och i företag som hör till dess konsolideringsgrupp. I anvisningen ger Finansinspektionen rekommendationer för rutinerna för riskhantering och övrig intern kontroll, vilka har fastställts i föreskrift 203.27. Principerna för rapportering och informationsförmedling behandlas mer detaljerat än övriga principer, eftersom Finansinspektionen inte har meddelat någon separat anvisning om dessa principer. Vad som i denna anvisning sägs om värdepappersföretag gäller i tillämpliga delar också värdepappersföretagets konsolideringsgrupp.

Innehåll	Sida
1 Inledning	2
2 Principer för ledarskaps- och kontrollkultur i värdepappersföretag.....	2
3 Principer för identifiering, analys, begränsning och kontroll av risker.....	3
4 Principer för kontrollåtgärder och åtskiljande av uppgifter.....	5
5 Principer för rapportering och informationsförmedling	5
6 Övervakning av funktionerna och avhjälpande av brister.....	8
6.1 Internrevisionens roll	8
6.2 Internrevisionens ställning	9

1 Inledning

Bristfällig intern kontroll har varit den viktigaste orsaken eller en betydande faktor i ett flertal av fallissemangen på finansmarknaden såväl i Finland som i utlandet. Finansinspektionen har därför ansett det nödvändigt att meddela en föreskrift och en anvisning om principerna för riskhantering och övrig intern kontroll. Principerna i föreskriften och anvisningen är allmänt vedertagna och ger uttryck för ett synsätt som är gemensamt för finansinspektionerna i olika länder.

I anvisningen används termerna riskhantering och övrig intern kontroll i samma betydelse som i Finansinspektionens separata föreskrift 203.27 (1.6.1999) om riskhantering och övrig intern kontroll i värdepappersföretag.

Den interna kontrollen består av en serie rutiner som är integrerade med verksamheten i enheten. Rutinerna är en del av ledningen av ett värdepappersföretag. I den interna kontrollen deltar hela personalen. I en liten organisation kan det vara svårt att följa principerna in i minsta detalj. Alternativa kontrollmetoder kan då komma i fråga. I sådana fall skall valet av styr- och kontrollrutiner beslutas separat av styrelsen.

2 Principer för ledarskaps- och kontrollkultur i värdepappersföretag

Värdepappersföretaget skall

- 1) bestämma värdepappersföretagets 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 värdepappersföretagets samtliga funktioner och är rätt dimensionerade i förhållande till riskerna i de olika verksamheterna.
 - I ett värdepappersföretags organisation är det önskvärt att det övergripande ansvaret för riskhanteringen koncentreras. Härigenom säkerställs att verksamheten i värdepappersföretaget och i dess konsolideringsgrupp följs upp och att riskerna i verksamheterna identifieras så att den högsta ledningen har uppgifter om den totala effekten av samtliga risker i affärsverksamheten på värdepappersföretagets och dess konsolideringsgrupps resultat och kapitalbas.
 - Om affärsstrategier och verksamhetsprinciper har fastställts för värdepappersföretagets konsolideringsgrupp, skall de värdepappersföretag som hör till konsolideringsgruppen separat fastställa sina egna affärsstrategier och verksamhetsprinciper.
 - Cheferna skall se till att befogenheterna och ansvaret har fastställts skriftligen.

-
- 2) fastställa kvantitativa och kvalitativa mål för varje delområde av värdepappersföretagets verksamhet samt kontrollera att målen uppfylls.
- Det skall i efterhand vara möjligt att av protokoll och bilagorna till protokoll verifiera vilka beslut som har fattats och hur kontrollen har skett.
 - Vid målsättning och belöning för måluppfyllelse skall hänsyn tas till den interna kontrollen och uppmärksammas att strävan efter måluppfyllelse inte inbjuder till oacceptabla förfaringssätt.
 - För att bibehålla förtroendet för värdepappersföretaget och värdepappersföretagets goda rykte och för att skydda värdepappersföretaget mot brottslig verksamhet och oegentligheter skall målsättningen och rutinerna bygga på etiskt godtagbara principer. Värdepappersföretaget skall fästa uppmärksamhet vid kundkretsens beskaffenhet och vinnlägga sig om att lära känna sina kunder, iaktta god sed på värdepappersmarknaden och följa bestämmelserna om förhindrande av penningtvätt.
- 3) säkerställa att personalen är kompetent och lämpad för sina arbetsuppgifter och har den information som behövs för att uppgifterna skall kunna utföras.
- Värdepappersföretaget skall se till att varje anställd är medveten om hur den interna kontrollen påverkar hans uppgifter och förbinder sig att följa principerna för intern kontroll.
 - I värdepappersföretaget skall finnas rutiner som förhindrar att inkompetenta eller oärliga personer anställs.
 - Vid köp av externa tjänster skall värdepappersföretaget vinnlägga sig om att iaktta samma omsorg som vid rekrytering av ordinarie personal. Detta skall gälla såväl det företag från vilket tjänsterna köps som de anställda i företaget som i samband med uppdraget får tillgång till värdepappersföretagets interna information. Detta kontrollansvar kan värdepappersföretaget inte föra över på det företag där tjänsterna köps.

3 Principer för identifiering, analys, begränsning och kontroll av risker

Värdepappersföretaget skall

- 4) försäkra sig om att riskerna i affärsverksamheten identifieras och analyseras.
- En adekvat riskhantering skall täcka (men inte vara begränsad till) åtminstone följande riskområden:

-
- Med **kreditrisk** avses risken att motparten inte kan svara för sina förbindelser gentemot värdepappersföretaget.
 - Med **marknadsrisk** avses risken att värdepappersföretaget gör förlust när marknadspriset eller volatiliteten i marknadspriset förändras i en för värdepappersföretaget ofördelaktig riktning. Marknadsriskerna är ränte-, valutakurs- och aktiekursrisker eller andra prisrisker (råvaruprisrisker).
 - Med **värdepappersföretagets finansieringsrisk** avses risken att värdepappersföretaget inte kan fullfölja sina betalningsskyldigheter.
 - Med **marknadslikviditetsrisk** avses risken att värdepappersföretaget inte kan realisera eller täcka sina positioner till rådande marknadspris, eftersom marknaden inte är tillräckligt likvid eller inte fungerar till följd av någon störning
 - Med **operativ risk** avses risken att brister i informationssystemet eller i andra system eller i interna kontroll- och säkerhetsrutiner medför oväntade förluster.
 - Med **legal risk** avses en risk som beror på ogiltiga kontrakt eller brist på dokumentation.
 - Med **strategisk risk** avses risken att den valda strategin är fel dimensionerad i proportion till värdepappersföretagets risktagningsförmåga, tekniska resurser eller personalens kompetens. Om så är fallet, kan den valda strategin visa sig vara en felsatsning och leda till ekonomiska förluster.
- 5) fastställa principer för riskexponeringen samt slå fast rutiner för riskbegränsningen och övervaka att de följs.
- Skriftliga rutiner för riskbegränsningen och limiter för kvantifierbara risker skall fastställas.
 - Riskhanteringen skall innefatta en beslutsordning för nya engagemang och nya produkter. Alla involverade bör i fråga om sina egna ansvarsområden vara medvetna om riskerna och riskhanteringen i den nya verksamheten.
 - Efterlevnaden av riskhanteringsrutinerna och limiterna skall fortlöpande kontrolleras. Avvikelser från riskhanteringsrutinerna och limitöverskridningar skall genast utvärderas och rapporteras. För avvikelsekontrollen skall tydliga rutiner utarbetas.
 - Riskhanteringsrutinerna och limiterna skall regelbundet ses över så att de överensstämmer med de fastslagna riktlinjerna och det rådande marknadsläget.

-
- 6) försäkra sig om att värdepappersföretaget har en riskkontrollfunktion som är oberoende av risktagningsfunktionen.
- Riskkontrollfunktionen skall vara oberoende av risktagningsfunktionen på alla nivåer i värdepappersföretaget inklusive styrelsen.

4 Principer för kontrollåtgärder och åtskiljande av uppgifter

Värdepappersföretaget skall

- 7) säkerställa att de interna kontrollrutinerna integreras med värdepappersföretagets dagliga rutiner och att farliga arbetskombinationer har delats upp på flera anställda och rutinerna för de viktigaste funktionerna har skriftligen dokumenterats.
- Ändamålsenlig kontroll skall vara integrerad med funktionerna på alla nivåer inom organisationen.
 - Kontrollrutinerna för de olika organisationsnivåerna omfattar bl.a.
 - styrelsens uppföljning av verksamheten och de uppsatta målen
 - ändamålsenlig kontroll av verksamheten i enheterna
 - fysiska kontroller
 - kontroll av limiterna och uppföljning av avvikelser
 - rutiner för godkännande och befullmäktigande så att den följande organisationsnivån alltid informeras om överskridningar av limiterna
 - säkerhets- och avstämningsrutiner och rapportering av avvikelser till den ansvariga organisationsnivån.
- 8) säkerställa att anställda som representanter för värdepappersföretaget inte handlägger affärstransaktioner som berör dem själva eller personer i deras närmaste krets eller på annat sätt deltar i beslut om sådana transaktioner.
- Ledningens och personalens bindningar och bisysslor skall utredas och registreras så att eventuella konfliktsituationer undviks. Uppgifterna i registret skall uppdateras.

5 Principer för rapportering och informationsförmedling

Redovisnings- och informationssystemen genererar information om affärstransaktionerna i ett värdepappersföretag och händelserna på marknaden för det interna beslutsfattandet, för den interna kontrollen och för externt bruk. Informationen skall ge en rättvisande bild av verksamheten i värdepappersföretaget. Därför skall värdepappersföretaget

-
- 9) säkerställa att det har adekvata redovisnings- och informationssystem till stöd för beslutsfattandet och utvärderingen av verksamheten.
- Varje transaktion redovisas fullständigt och riktigt, i rätt tid, tillräckligt specificerat och utan dröjsmål.
 - Verifieringskedjan skall vara obruten ända från det ursprungliga dokumentet.
 - Det skall finnas en skriftlig beskrivning av värdepappersföretagets redovisningssystem som inbegriper både den manuella och den elektroniska hanteringen samt rutinerna för den interna kontrollen.
 - Ledningen och den övriga personalen skall snabbt få sådan tillförlitlig och ändamålsenlig information som den behöver för att kunna sköta sina uppgifter. Informationen skall vara relevant och adekvat med tanke på beslutsfattandet.
 - Myndigheterna får sina rapporter snarast möjligt och inom utsatt tid.
 - Den externa informationen (bokslut, rapporter till tillsynsmyndigheterna osv.) följer lagar och bestämmelser.
 - Ledningen skall inom organisationen skapa lämpliga informationskanaler där informationen går i bägge riktningarna.
- 10) säkerställa att värdepappersföretaget har adekvata och ändamålsenliga datasystem.
- Värdepappersföretaget skall ha den kompetens, organisation och interna kontroll som behövs för att lagra och hantera data i maskinläsbar form. För den interna kontrollen innebär det att principerna under punkterna a – k nedan skall följas. De skall följas också i de fall databehandlingen delvis har decentraliserats till affärsenheter utanför IT-avdelningen. Värdepappersföretaget skall också se till att de företag som anlitas för data-tjänster tillämpar liknande principer.
 - I sin egen verksamhet skall värdepappersföretaget följa principerna nedan endast i den mån det driver ifrågavarande verksamhet. Egna riktlinjer och standarder för systemutveckling behöver således inte utarbetas om värdepappersföretaget endast använder färdigköpta program eller program som beställts kollektivt av flera värdepappersföretag och utvecklats enligt standarder som specificerats centralt.
 - 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, standarder-

-
- na, 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 systemutvecklingen och för systemens funktion, medan användarna svarar för att behandlade data är riktiga.
 - d) Systemutveckling och datadrift separeras så att de anställda i dessa funktioner har direkt åtkomst till varandras data endast via kontrollerade standardrutiner.
 - e) Värdepappersföretaget skall se till att internrevisionen har kompetens att utvärdera de interna IT-kontrollerna vad gäller ändamålsenlighet och funktionsförmåga.
 - f) Metoder för systemering och kvalitetssäkring skall utarbetas och upprätthållas 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 och godkännande av program- och maskinvara eller för ingående av kontrakt med leverantörerna skall utarbetas för att säkerställa att nyanskaffningar och kontrakt motsvarar värdepappersföretagets behov och fastställda standarder och garanterar fortlöpande service.
 - h) kontrollmekanismer och revisionsspårning skall byggas in i data-systemen 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. Åtkomsten till data och program skall på teknisk väg (genom användarnamn, lösenord osv.) begränsas till behöriga användare och överträdelser skall rapporteras och undersökas.
 - j) Risken för systemavbrott (brand, översvämning, elavbrott osv.) skall minimeras med hjälp av rutiner och riktlinjer för den fysiska säkerheten, och åtkomsten till känsligt material (datautrustning, datamedier, dokument osv.) skall begränsas till behöriga personer.
 - 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.

6 Övervakning av funktionerna och avhjälpande av brister

Effektiviteten i den interna kontrollen i värdepappersföretaget skall fortlöpande ses över. Övervakningen av större risker skall vara integrerad med de dagliga rutinerna. Affärsverksamheten skall också utvärderas regelbundet. För dessa behov skall värdepappersföretaget

- 11) säkerställa att internrevisionen är organiserad på ett ändamålsenligt sätt och att den fungerar enligt god revisionsledning.
 - Det är önskvärt att värdepappersföretaget tillämpar den centrala normuppsättningen yrkesstandarder för god intern revisionsledning, såsom de standarder som The Institute of Internal Auditors har gett ut.
- 12) säkerställa att styrelsen delges alla viktiga observationer som görs av interna och externa revisorer och av myndigheter.
 - Observationerna och de åtgärder som de ger anledning till skall i efterhand kunna verifieras med protokoll och bilagorna till protokoll.
- 13) se över den interna kontrollen och riskhanteringssystemen regelbundet och alltid när
 - värdepappersföretaget inleder verksamhet på en ny marknad
 - värdepappersföretaget 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.

6.1 Internrevisionens roll

Internrevisionen är en oberoende stabsfunktion som är underställd den högsta ledningen och har som uppgift att undersöka och utvärdera det interna kontrollsystemet vad gäller dimensionering och effektivitet samt de interna kontrollrutinernas kvalitet. Värdepappersföretaget skall organisera internrevisionen så att de uppgifter som hör till internrevisionen blir utförda. Internrevisionen skall arbeta enligt god intern revisionsledning.

En självständig intern revisor skall utses eller en avdelning för internrevision inrättas i värdepappersföretag som på grund av sin storlek, affärsrörelse och risktagning är skyldiga att göra det. I stället för en egen internrevision kan värdepappersföretaget också anlita externa, oberoende revisorer.

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

Även om målen och uppgifterna för internrevisionen kan variera i de olika värdepappersföretaget anses följande uppgifter i regel höra till internrevisionen:

- Internrevisionen skall granska tillförlitligheten och enhetligheten i den ekonomiska och operativa informationen och metoderna för identifiering, mätning, kategorisering och rapportering av sådan information.
- Internrevisionen skall granska de metoder som tillämpas för att säkerställa att verksamhetsprinciper, planer, metoder, lagar och bestämmelser med stor betydelse för verksamheten och rapporterna följs och kontrollera att organisationen följer dem.
- Internrevisionen skall granska de metoder som tillämpas för att trygga tillgångarna och i tillämpliga delar säkerställa att tillgångarna existerar.
- Internrevisionen skall utvärdera om resurserna används ekonomiskt och effektivt.
- Internrevisionen skall granska både den operativa verksamheten och olika projekt för att försäkra sig om att resultaten motsvarar de uppsatta målen samt kontrollera att verksamheten och projekten genomförs planenligt.
- Internrevisionen skall granska/utvärdera hanteringen av riskhanteringssystemens funktion.

Värdepappersföretagets ledning skall se till att dessa för den interna kontrollen så viktiga uppgifterna blir utförda.

6.2 Internrevisionens ställning

Följande allmänna principer gäller för den interna revisionsfunktionen:

- Den skall vara oberoende i förhållande till den granskade verksamheten.
- Dess verksamhetsområde skall vara obegränsat för att säkerställa att alla funktioner i värdepappersföretaget omfattas av granskningen.
- Den skall vara rätt dimensionerad i förhållande till värdepappersföretagets storlek och verksamhet och ha den kompetens och erfarenhet som behövs.
- Den skall ha en ställning i organisationen som säkerställer att granskningsrapporterna och rekommendationerna behandlas på ett behörigt sätt i styrelsen och i det eventuella förvaltningsorgan som övervakar styrelsens verksamhet.

Närmare upplysningar lämnas av: Kapitalmarknadsavdelningen