2013-12-16

Dnr 01.08.02. 2013/644

Finansinspektionen
Box 7821
103 97 Stockholm

Svar på remiss angående förslag till nya regler om hantering av operativa risker samt nya regler om it-system, informationssäkerhet och insättningssystem i kreditinstitut och värdepappersbolag

FI Dnr 11-11528,12-4167

Inledning och sammanfattning

Riksgäldskontoret ser positivt på Finansinspektionens förslag till nya regler om hantering av operativa risker samt it-system, informationssäkerhet och insättningssystem i kreditinstitut och värdepappersbolag. I likhet med Finansinspektionen och IMF ser Riksgälden ett behov av tydligare reglering för att öka företagens förutsättningar att identifiera, mäta och bedöma operativa risker.

Det finns tre avsnitt i föreskrifterna inom vilka Riksgäldskontoret önskar lämna synpunkter, dessa gäller styrning och ansvar, incidenter samt mål och inriktning för informationssäkerhet.

Finansinspektionens föreskrifter och allmänna råd om hantering av operativa risker

2 kap. Styrning och ansvar, 1 §

Det finns bland finansiella aktörer delade uppfattningar om begreppen riskaptit och risktolerans samt huruvida innebörden bör ses som densamma eller inte. Riksgäldskontoret anser, i enlighet med bland annat Committee of Sponsoring Organizations of the Treadway Commission (COSO), att detta är två skilda begrepp.[1] Under 2 kap. Styrning och ansvar behandlar Finansinspektionen endast begreppet risktolerans. I syfte att undvika missförstånd föreslår Riksgäldskontoret att även begreppet riskaptit omnämns i sammanhanget eftersom även riskaptiten bör vara dokumenterad och beslutad av styrelsen. Denna komplettering skulle även bidra till att tydliggöra att begreppen relaterar till två skilda definitioner.

3 kap. Identifiering och mätning, Incidenter, 6 §

Riksgäldskontoret välkomnar att Finansinspektionen föreskriver om incidenter då detta är ett viktigt verktyg för att hantera operativa risker. Ett vanligt tillvägagångssätt inom incidenthantering är att anställda skickar in så kallade incidentrapporter till en central funktion som behandlar dessa. I 6 § anges att ett företag ska ha rutiner för att säkerställa att dokumenterade uppgifter är korrekta. Detta skulle kunna tolkas som att riktigheten i varje enskild incidentrapport måste kunna fastställas. En sådan tolkning kan skapa problem för de företag som ser fördelar i att även kunna ta emot anonyma incidentrapporter. Riksgäldskontoret föreslår därför en omformulering eller ett förtydligande av denna mening i syfte att möjliggöra för dessa företag att fortsätta erbjuda anonym incidentrapportering.

[1] Trots problematiken att European Banking Authority (EBA) inte särskiljer begreppen hålls de skilda åt i många andra betydande risksammanhang och Riksgäldskontoret anser därför att det är mer lämpligt att utgå från andra instansers och ramverks definitioner. Riksgäldskontoret anser därmed att de definitioner som Finansinspektionen angav i remissexemplaret om föreskrifter och allmänna råd om styrning, riskhantering och kontroll i kreditinstitut var relevanta.

Finansinspektionens föreskrifter och allmänna råd om it-system, informationssäkerhet och insättningssystem

3 kap. Informationssäkerhet, Mål och inriktning, 2 §

I paragraf 2 anges att ”ett företag ska fastställa och dokumentera mål och inriktning med sitt informationssäkerhetsarbete. Styrelsen eller den verkställande direktören ska besluta om målen och inriktningen på informationssäkerhetsarbetet”.

Riksgäldskontoret föreslår följande tillägg: ”Företagets ledning ska löpande informera sig om arbetet med informationssäkerhet samt minst en gång per år följa upp och utvärdera informationssäkerhetsarbetet på företaget”.