Protokollsbilaga G
Direktionens protokoll 130131, §13b

Rapport ISK 2012

DATUM: 2013-01-24
AVDELNING: STA/RIE
HANDLÄGGARE: Jeanette Eklöf

SVERIGES RIKSBANK
SE-103 37 Stockholm
(Brunkebergstorg 11)

Tel +46 8 787 00 00
Fax +46 8 21 05 31
registratorn@riksbank.se
www.riksbank.se

DNR 2011-789-STA

Intern styrning och kontroll i Riksbanken 2012- underlag för direktionens bedömning

Bakgrund

Direktionen ska enligt riksbankslagen 10 kap. 3 § lämna en bedömning av om den interna styrningen och kontrollen (ISK) vid Riksbanken är betryggande. Denna rapport sammanfattar arbetet med intern styrning och kontroll på Riksbanken under 2012, och utgör underlag för direktionens bedömning. Rapporten innehåller:

- En beskrivning av Riksbankens process för intern styrning och kontroll, inklusive de åtgärder som genomförts under 2012 för att förbättra processen.
- En beskrivning av de riskbegränsande åtgärder som genomförts under 2012.
- En sammanfattning av de incidenter som rapporterats under 2012.
- En redogörelse för resultatet av självutvärderingen av intern styrning och kontroll per december 2012.

Riksbankens process för intern styrning och kontroll

Av Riksbankslagens 9 kapitel 1a§ följer att:

Direktionen ansvarar för verksamheten och ska se till att den bedrivs effektivt och enligt gällande rätt, att den redovisas på ett tillförlitligt och rättvisande sätt samt att Riksbanken hushållar väl med statens medel.

Direktionen ska säkerställa att det vid Riksbanken finns en intern styrning och kontroll som fungerar på ett betryggande sätt.

Med intern styrning och kontroll avses den process som syftar till att Riksbanken med rimlig säkerhet fullgör de krav som framgår av första stycket. I denna process ska ingå momenten riskanalys, kontrollåtgärder, uppföljning och dokumentation.

Riksbankens process för intern styrning och kontroll har utformats enligt följande:

Kontrollmiljö

Direktionen är ytterst ansvarig för intern styrning och kontroll på Riksbanken. De beslutar om Riksbankens instruktion, där ansvaret inom organisationen tydliggörs. De beslutar också om Riksbankens övergripande interna regelverk. Ansvaret för den dagliga styrningen och kontrollen av verksamheten, dess effektivitet, resultat och riskhantering ligger hos avdelningscheferna som i sin tur rapporterar till direktionen. Alla medarbetare har ansvar för att påtala risker och att rapportera incidenter i verksamheten.

Den styrmodell som tillämpas på Riksbanken innebär att verksamheten styrs mot en övergripande vision och mot strategiska mål som formulerats utifrån Riksbankens uppdrag.

Riskanalys

Riksbanken arbetar systematiskt med riskhantering och har en bankgemensam process för hantering av operativa risker. Riskerna identifieras och värderas enligt samma modell i hela verksamheten. Modellen baseras på ESCB:s "operational risk management framework". Riskansvaret är kopplat till verksamhetsansvaret och riskanalyser genomförs som ett led i verksamhetsplaneringen. Riskägaren beslutar för varje risk om den ska accepteras, begränsas eller undvikas. Riskhantering och verksamhetsplanering är integrerade genom en samordnad process för dokumentation och uppföljning.

Riskhanteringen avseende operativa risker styrs av en policy och en mer detaljerad regel för hantering av operativ risk. Regeln sammanfattar Riksbankens process för riskhantering och tydliggör ansvar och roller. Även för hantering av finansiella risker finns ett riskramverk som gäller för hela banken. Riskenheten på stabsavdelningen stödjer Riksbankens verksamheter med ramverk, metoder och rådgivning inom alla riskområden.

Kontrollåtgärder

För att upprätthålla en låg risknivå i befintliga processer och rutiner finns olika typer av förebyggande kontroller i form av ansvars- och arbetsfördelning, attestregler och inbyggda kontrollfunktioner i IT-system, eller efterhandskontroller i form av exempelvis avstämningar och utfallsanalyser. Många av dessa kontroller finns dokumenterade i rutinbeskrivningar. Andra kontroller utgör så kallade resultatindikatorer och följs upp som en del av den tertialvisa uppföljningen av verksamheten. För att begränsa eller undvika nya operativa risker som uppmärksammas tas handlingsplaner fram i samband med verksamhetsplaneringen eller löpande, om riskerna kräver omedelbar hantering.

Uppföljning

Måluppfyllnaden följs upp för Riksbankens olika målområden varje tertial via så kallade resultatindikatorer och handlingsplaner. Även riskerna följs upp per tertial, dels per målområde och dels för Riksbanken som helhet.

Processen för intern styrning och kontroll utvärderas årligen enligt en modell som bygger på COSO-ramverkets fem komponenter: kontrollmiljö, riskhantering, kontrollaktiviteter, information och kommunikation samt uppföljning och utvärdering[1]. Utvärderingen sker mot ett antal kriterier som bland annat anger hur arbetet ska vara organiserat, vilka styrdokument som ska finnas på plats och hur metoder, modeller och processer ska vara utformade.

Internrevisionen gör en oberoende utvärdering av den interna styrningen och kontrollen i verksamheten genom granskningar enligt en årlig plan som fastställs av direktionen.

Dokumentation och rapportering

Verksamhetens handlingsplaner, resultatindikatorer och risker dokumenteras per målområde i Riksbankens IT-stöd för verksamhetsplanering- och uppföljning: RYC. Handlingsplanerna dokumenteras och följs upp samordnat, oavsett om de primärt syftar till att hantera risker eller inte. RYC möjliggör även full spårbarhet mellan Riksbankens övergripande risker och varje enskild risk inom respektive målområde.

Verksamhetsuppföljningen sammanställs och rapporteras per tertial. . Måluppföljningen redovisas även i årsredovisningen. Uppföljningen av riskerna rapporteras varje tertial i en riskrapport som innehåller riskenhetens oberoende bedömning av verksamhetens finansiella och operativa risker på en övergripande nivå.

Utvärdering av processen för intern styrning och kontroll dokumenteras i en PM för var och en av de fem COSO-komponenterna.

Internrevisionens granskningar dokumenteras i en rapport för varje granskning.

Direktionen har, utöver denna rapport, under 2012 fått följande rapportering som underlag för sin bedömning av intern styrning och kontroll:

- Uppföljning av 2012 års verksamhetsplan, tertialvis.
- Rapportering av Riksbankens finansiella och operativa risker, tertialvis.
- Utvärdering av intern styrning och kontroll, i juni 2012.
- Rapportering från internrevisionen, löpande under året.

[1] För mer information om COSO och Riksbankens utvärderingsmodell, se PM Utvärdering av intern styrning och kontroll på Riksbanken 2012- bakgrund och sammanfattning (dnr 2011-789-STA)

Förbättringsåtgärder 2012 avseende processer för intern styrning och kontroll

Under 2012 har olika åtgärder genomförts för att förbättra de processer som stödjer en god intern styrning och kontroll:

En formaliserad rutin har tagits fram för Riksbankens årliga översyn av Riksbankens arbetsordning och instruktion.

Den nya strategiska plan som togs fram 2011 implementerades under 2012, vilket gett en ökad tydlighet i planeringsprocessen. Användarna av Riksbankens IT-stöd för verksamhetsplanering har under året fått extra stöd och utbildning vilket förbättrat strukturen på planering, riskhantering och uppföljning.

De nya regler för hantering av operativ risk samt för verksamhetsplanering- och uppföljning som togs fram 2011 har under 2012 utvärderats och reviderats. Revidering pågår även av flera andra regler och nya versioner beräknas finnas på plats under första kvartalet 2013.

Den compliancefunktion som direktionen beslutade om 2011 har etablerats under året och en plan för funktionens arbete under 2013 har presenterats för direktionen. Alla nyanställda får sedan i september en introduktion till compliance och Riksbankens interna regelverk i syfte att minska risken för regelöverträdelser. En obligatorisk utbildning i riskmedvetenhet, som vände sig till alla medarbetare, har även genomförts under året. För att öka tillgängligheten till Riksbankens interna regelverk har ett nytt gränssnitt tagits fram för att presentera regelverket på Banconätet.

Den process för IT-säkerhet som infördes på Riksbanken 2011 utvärderades i april 2012. En översyn av katalogen med IT-säkerhetsåtgärder påbörjades därefter och kommer att fortsätta under 2013 samordnat med projektet för utkontraktering av Riksbankens IT-drift.

För att utvärdera och stärka Riksbankens krisberedskap genomfördes en kombinerad larm- och reservanläggningsövning i februari. Övningen visade att larmningen fungerade bra och att personalen kunde utföra sina arbetsuppgifter från reservanläggningen i Strängnäs. De förbättringsåtgärder som identifierades under övningen avsåg mindre justeringar i IT-stödet och har åtgärdats under året.

En fördjupad kartläggning av Riksbankens huvudprocesser (de processer i vilka Riksbankens uppdrag genomförs) påbörjades under hösten 2012 och fortsätter under 2013. Kartläggningen utgör dels underlag för en processbaserad informationsstruktur i Riksbankens nya diarie- och arkivsystem och dels för en beskrivning den interna kontrollstrukturen som utgår från Riksbankens processer.[2] Som en del av processdokumentationen upprättas ett dokument om intern styrning och kontroll för respektive process.

[2] Riksbanken har – inom ramen för sitt arbete med att förbättra intern styrning och kontroll- blivit rekommenderad av både riksrevisionen och internrevisionen att under 2012 kartlägga och beskriva kontrollstrukturen i sina huvudprocesser/mest kritiska processer.

Riskhantering avseende operativa risker under 2012[3]

Operativa risker uppstår när Riksbanken utför sina uppdrag och finns därmed i hela verksamheten såväl i det dagliga löpande arbetet som i pågående förändringsaktiviteter. Risk innebär osäkerhet om framtida händelser och deras negativa effekter på Riksbankens verksamhet, tillgångar eller anseende.

En mycket viktig förutsättning för att Riksbanken framgångsrikt ska kunna utföra sina huvuduppgifter är att marknaden och allmänheten har ett högt förtroende för Riksbanken. Riksbankens vision är att vara "bland de bästa" när det gäller kvalitet och effektivitet för att behålla ett högt förtroende. Riksbanken måste därför ha god förmåga att snabbt kunna identifiera och hantera händelser i omvärlden och en väl fungerande extern kommunikation. Det gäller allt från att hantera en förändrad hotbild mot exempelvis kontantverksamheten eller IT-stödet till att anpassa processer och IT-stöd till nya förutsättningar.

Verksamhetens riskanalyser avseende operativa risker inför 2012 visade endast på mindre förändringar jämfört med året innan. Sammantaget visade riskanalyserna på behov av att hantera risker relaterade till otydlig kommunikation- framför allt kring det penningpolitiska beslutet, stabilitet och säkerhet i IT-miljön, hantering av konfidentiell information, samt beroenden av nyckelpersoner och externa parter. För att stärka beredskapen för framtida förändringar identifierades också behov av att stärka intern kontroll både i bankövergripande interna processer och i vissa verksamhetsspecifika processer. Under 2012 påverkades risknivån även av den pågående IT-utkontrakteringen.

Policyverksamheten

Riksbankens policyverksamhet innefattar penningpolitik och finansiell stabilitet. För att begränsa risken för ett sänkt förtroende är det viktigt att penningpolitiken är transparent och trovärdig och att Riksbanken är öppen och tydlig i sina bedömningar av den finansiella stabiliteten.

För att minska risken för otydlighet i beslutsunderlaget för det penningpolitiska beslutet, har flera olika aktiviteter pågått under 2011 -2012. De flesta av åtgärderna förväntas få genomslag under 2013. En annan viktig riskhanterande aktivitet var utvecklingen av ett nytt databibliotek, som både möjliggör spårbarhet och en mer strukturerad hantering av data. En första version av databiblioteket togs i bruk i oktober 2012. Parallellt med den fortsatta utvecklingen av databiblioteket genomförs ett implementeringsprojekt som även ser över en enhetlig standard för programvaror och rutiner. Båda projekten fortsätter under 2013.

Inom området finansiell stabilitet har Riksbankens ökade internationella engagemang inneburit att nya arbetsuppgifter och därmed nya risker tillkommit. Riksbanken förväntas inom detta område ofta ta ställning i olika frågor med mycket kort varsel, vilket ger begränsad tid för kvalitetssäkring och mötesförberedelser. De åtgärder som vidtagits under 2012 är ett ökat fokus på internationellt regleringsarbete, ökad

[3] För mer information om risker och handlingsplaner hänvisas till Riksbankens verksamhetsplan och verksamhetsuppföljning, samt IT-stödet RYC.

- samverkan internt och med andra berörda myndigheter samt resursförstärkningar. Andra aktiviteter som genomförts under året i syfte att stärka upp interna processer är inrättandet av en ny enhet för makrotillsyn, översyn av processen för att ta fram den finansiella stabilitetsrapporten, samt åtgärder för att förbättra styrning, uppföljning och genomförande av projekt och handlingsplaner.

  Både avdelningen för penningpolitik och avdelningen för finansiell stabilitet har under året arbetat med kompetensspridning och arbetsrotation i syfte att minska personberoendet.

Operativ verksamhet:

Riksbankens operativa verksamhet innefattar betalningsförmedling, kapitalförvaltning, kontanthantering och statistikproduktion.

Inom betalningsförmedlingen är den allvarligaste risken att betalningssystemets (RIX) funktion inte kan upprätthållas. Konsekvensen skulle kunna bli stora störningar i det finansiella systemet och samhället i stort samt ett försämrat förtroende för Riksbanken. Ökade transaktionsvolymer har ökat risknivån vid ett eventuellt användande av manuella reservrutiner. Fokus under 2012 har därför varit att behålla driftsmiljön stabil, att öka motståndskraften i systemet genom förbättring och övning av rutiner i samarbete med RIX-deltagarna samt att utreda möjligheten till utveckling av nya kontinuitetslösningar. Förslag till alternativ till manuella reservrutiner har diskuterats med deltagarna och kommer att fortsätta utredas under 2013.

Under 2012 har förberedelser genomförts för att under 2013 uppgradera RIX och eventuellt byta ut nuvarande systemstöd för hantering av säkerheter. Därutöver har nya rutiner tagits fram och dokumenterats för ärendehantering vid programändringar, lösenordshantering och logguppföljning.

Inom kapitalförvaltningen och kontanthanteringen finns inneboende risker till följd av att stora belopp hanteras i kapitalflöden och kontanter.

Inom kapitalförvaltningen inleddes 2011 en större översyn av regler, rutiner och arbetsbeskrivningar i syfte att stärka de interna processerna. . Översynen har slutförts under 2012 och det finns nu även en årlig rutin på plats för att upprätthålla en årlig revidering. För att kunna minska antalet egenutvecklade lösningar och manuella handgrepp har ny funktionalitet införts i systemstödet för kapitalförvaltning. Därutöver har en mer driftssäker hämtning av dagliga marknadspriser för värdering införts.

Inom kontanthanteringen pågår två stora projekt för att öka säkerheten och minska risken för rån och angrepp respektive förfalskning. Dels byggs ett nytt kontanthanteringskontor (Broby) som ska tas i drift under andra halvåret 2013 och dels ska en ny sedel- och myntserie införas från 2015. Inför förändringarna i kontanthanteringen har en genomgång gjorts av verksamhetsprocesserna och alla rutinbeskrivningar har setts över. Inom båda projekten genomförs riskanalyser kontinuerligt och riskhantering har en central roll i alla delar av projekten.

- Personberoendet inom de operativa verksamheterna har minskat genom att de åtgärder som inleddes under 2011 slutförts och fått genomslag under 2012. Inom samtliga enheter har ett systematiskt arbete genomförts för att bredda kompetensen och säkerställa ersättare vid frånvaro. På statistikenheten har strukturen inom enheten setts över och nyrekryteringar har gjorts för att hantera nya arbetsuppgifter och underlätta pensionsavgångar. Även RIX-enheten har nyrekryterat för att möta pensionsavgångar. Inom kapitalförvaltningen har vissa personalomställningar gjorts och inom kontantförsörjningen har kompetens till det nya kontanthanteringskontoret säkrats genom att personal från de båda nuvarande kontoren tackat ja till att följa med till Broby.

Bankgemensamma områden

Policyverksamheten och den operativa verksamheten stöds och samordnas genom olika interna processer, som är grupperade i sex bankgemensamma områden: kommunikation, medarbetare, ledning och styrning, IT, administrativt stöd och service samt miljö.

Risknivån inom stödverksamheten påverkades under 2012 framför allt av den pågående IT-utkontrakteringen. För att begränsa riskerna i projektet har särskilda HR-insatser genomförts, förändringar i IT-miljön har begränsats och resursförstärkning har gjorts genom konsulter. Hanteringen av risker i IT-miljön har påverkats genom att förbättringsåtgärder måste samordnas med tidplanen för utkontrakteringen. Samarbetet med EVRY ger Riksbanken nya tekniska förutsättningar att minska riskerna i IT-miljön framöver, bland annat när det gäller avbrottshantering. Risken för ett avbrott i den externa tele- och datakommunikationen har begränsats under 2012 genom att ytterligare en fiberförbindelse kopplades in till Riksbankshuset i maj.

Insatser har även gjorts för att förbättra Riksbankens kommunikation med allmänheten och andra målgrupper. Bland annat har den externa webben uppgraderats och webbplatsen har gjorts mer pedagogisk och användarvänlig. Målet är att öka förståelsen för Riksbankens uppdrag och därigenom behålla ett högt förtroende. Satsningar har även gjorts för att öka dialogen med olika målgrupper.

Inom personalområdet fortsatte satsningarna på att upprätthålla ett gott arbetsklimat och att stärka Riksbankens varumärke som arbetsplats. Målet är att både kunna rekrytera och behålla kompetenta medarbetare.

Bankövergripande risker

Vissa risker finns inom hela Riksbankens verksamhet och behöver därför hanteras med bankövergripande handlingsplaner. En sådan risk är att konfidentiell information sprids till obehöriga. Risken bedöms inom flera delar av verksamheten kunna få allvarliga konsekvenser, framför allt för Riksbankens anseende. Under 2012 har en aktivitet påbörjats som innebär att dels revidera Riksbankens regel för hantering av information och dels att genomföra en ny klassificering av Riksbankens information. Regeln ska skrivas om för att göra den tydligare och lättare att förstå och därmed tillämpa. En förutsättning för att kunna klassificera informationen är att den

- kartläggs, vilket görs samordnat med förberedelserna för Riksbankens nya diarie- och arkivsystem. Aktiviteten kommer att slutföras under 2013 genom att hela verksamheten utbildas i informationshantering. Det nya diarie- och arkivsystemet är planerat att vara på plats under 2013 och syftar bland annat till att underlätta för Riksbanken att uppfylla offentlighetsprincipen.

Incidenthantering

Sedan 2011 har Riksbanken en ny bankgemensam incidentrapporteringsprocess. En gemensam incidenthistorik gör det möjligt att lära av tidigare incidenter och ökar Riksbankens möjlighet att genomföra effektiva förbättringsåtgärder. Incident-historiken används också som ett stöd i riskanalyserna.

Under 2012 rapporterades 88 incidenter, att jämföra med 89 under 2011. Ingen av incidenterna medförde några allvarliga konsekvenser för Riksbanken och verksamheten har tagit fram åtgärdsplaner där de bedömt att det är nödvändigt. De mest uppmärksammade incidenterna påverkade den externa webben och RIX-systemet.

Den incident som haft störst påverkan på betalningsförmedlingen inträffade i augusti. Verksamheten drabbades då av ett avbrott under cirka två timmar på grund av ett fel i Riksbankens utrustning för kommunikation med SWIFT som medförde att betalningar inte kunde genomföras. I november inträffade en incident som visade att det var möjligt att ge kredit utan säkerhet till en deltagare i RIX. Orsaken var en felaktig systemuppsättning mellan RIX och Riksbankens system för hantering av säkerheter. Åtgärder har vidtagits för att minska risken för att det händer igen, och det pågår även en utredning för att identifiera eventuella ytterligare brister i systemen.

I oktober drabbades Riksbanken och flera andra organisationer av riktade överbelastningsattacker mot sina webbplatser. Attackerna mot Riksbanken ledde till att webben låg nere till och från under några dagar. Efter det har tekniska lösningar införts som gör det svårare att slå ut webbplatsen. Attackerna innebar också att Riksbankens beredskap för alternativa publiceringsvägar testades i "skarpt" läge.

Exempel på övriga incidenter som rapporterats under året är avbrott under riksbankschefens chatt efter räntebeskeden i februari och maj, avbrott och kvalitetsbrister i telefonin, strömavbrott och hissproblem på kontanthanteringskontoren, samt felaktig hantering av konfidentiell information. Även olika typer av handläggningsfel har rapporterats, till exempel har felaktig information publicerats och felregistreringar i olika system har gjorts både internt och av externa parter.

Tolv av de 88 incidenterna innebar kostnader för banken, utöver förlorad arbetstid. Ingen incident kostade mer än 100 000 SEK, men tre av dem kostade mellan 10 000 och 100 000 SEK. Dessa incidenter var en stöld av en riksbanksdator vid ett inbrott i en privatbostad, byte av lås i valv på grund av att nycklar saknades samt en skada på kylsystemet som ledde till vattenskada. Mer än hälften av incidenterna orsakade merarbete och tolv bedömdes ta mer än tio timmar att hantera. Rapportörerna har

- bedömt att cirka en fjärdedel av incidenterna är av sådan karaktör att de skulle kunna leda till skada på Riksbankens anseende.

Internrevision[4]

Internrevisionen har under 2012 följt upp tidigare rapporter, vilket i många fall lett till att utestående iakttagelser har kunnat stängas. Kvarstående iakttagelser om brister finns främst inom kapitalförvaltningen, framtagning av den penningpolitiska rapporten, operativ ledning samt Riksbankens IT verksamhet.

Granskningarna under 2012 enligt beslutad revisionsplan har fokuserat på verksamhetens arbete med analys av banksektorn, översyn av mynthanteringen, Riksbankens personskydd samt framtagning av den penningpolitiska rapporten.

Vid årsskiftet 2012/2013 finns 17 kvarstående iakttagelser som bedöms som "otillfredsställande" och 31 kvarstående iakttagelser vilka bedöms som "tillfredsställande men bör förbättras". Handlings- och tidsplaner finns för samtliga iakttagelser. Samtliga kvarstående iakttagelser följs löpande upp av internrevisionsavdelningen.

Utvärdering av processen för intern styrning och kontroll

Processen för intern styrning och kontroll har utvärderats mot nivån "etablerad ISK". Nivån innebär att processerna för intern styrning och kontroll är tillräckligt omfattande och strukturerade för att ISK ska anses vara betryggande, men att det fortfarande finns utvecklingspotential.

Målnivån för 2012 var densamma som 2011 och uppnåddes för 17 av 19 områden. Inom områdena lagefterlevnad respektive generella IT-kontroller är två utvärderingkriterier fortfarande endast delvis uppfyllda, vilket beror på att åtgärder inom dessa områden tar tid att införa. Det som saknas är dels en strukturerad process för att kontrollera efterlevnaden av lagar och regler och dels att genomföra regelbundna återläsningstester för IT-miljön som helhet.

I juni 2012 lämnade riskenheten ett förslag på lämplig framtida målnivå för ISK. Den inriktning som valdes innebär att Riksbanken fortsätter att utveckla sina ISK-stödjande processer och strävar mot att uppnå nivån "avancerad ISK" (nivå 4) under 2013. Nivån "avancerad" innebär att processerna för ISK är etablerade och väl fungerande. Innan en slutlig målnivå fastställs ska utvärderingskriterierna ses över och revideras. Orsaken är att det vid utvärderingarna har visat sig att det finns kriterier som, i sin nuvarande exakta ordalydelse, inte är helt relevanta för Riksbanken. Det finns också kriterier som är tolkningsbara, vilket gör att det är svårt att bedöma om de är helt eller delvis uppfyllda.

För att kunna bedöma hur ISK utvecklas under året har utvärderingen för 2012 även gjorts mot nuvarande kriterier på nivå 4. Utvärderingen visar att nivån "avancerad" varit uppnådd för tio av 19 områden under hela 2012.

[4] Detta avsnitt har skrivits av Kristina Hirschfeldt/IR