Till
Direktionen för
Riksbanken

Rapport

Extern kvalitetssäkring av Internrevisionen vid Riksbanken

Bakgrund och syfte

Internrevisionen vid Riksbanken ska granska och bedöma intern styrning och kontroll samt riskhantering och därutöver bidra till effektivisering och förbättringar av bankens styrning och ledning. Analysen ska omfatta all verksamhet och granskningsobjekten ska väljas utifrån begreppen risk och väsentlighet.

Utanför det revisionsmandat som IR har ligger direktionsledamöternas utövande av tjänst, vilket granskas av fullmäktiges revisionsenhet.

Styrande för internrevisionens arbete är ”Riksbankens policy för Internrevision” (Policy) vilken är fastställd av Riksbankens direktion 2010-12-08. Policyn hänvisar till god sed på området, vilket bland annat uttrycks i revisionsstandarder och etiska koder publicerade av the Institute of Internal Auditors (IIA), och Information Systems Audit and Control Association (ISACA).

Enligt IIA:s Riktlinjer för Yrkesmässigt utövande av internrevision ska Kvalitetssäkrings- och kvalitetsförbättringsprogrammet omfatta såväl intern som extern utvärdering där den externa utvärderingen ska ske minst en gång vart femte år. Riksbanken genomförde en extern kvalitetssäkring första gången 2006.

PwC fick under hösten 2011 uppdraget att genomföra en förnyad extern kvalitetssäkring av Riksbankens internrevision. Uppdraget har utförts av Hans Löfgren, Fredrik Söder och Charlotte Eklund under tidsperioden oktober-december 2011.

Genomförande

Målet med uppdraget var att genomföra en extern kvalitetssäkring av Riksbankens internrevision i enlighet med Riktlinjer för yrkesmässig internrevision (the Institute of Internal Auditors Standards) för att därvid kunna

- uttala sig om internrevisionens efterlevnad av IIA:s Riktlinjer för yrkesmässigt utförande av internrevision samt
- genomföra en analys av förbättringsområden för internrevisionen med hänsyn till god internationell sed och IIA:s Riktlinjer

Vi har intervjuat Riksbankschefen, vice Riksbankschefen, chefen för avdelningen Finansiell Stabilitet, internrevisionschefen samt två internrevisorer på Riksbankens internrevision. Personer som bidragit med information finns redovisade i Bilaga 2.

Vi har även tagit del av granskningsdokumentation samt rapport från ett granskningsprojekt som genomförts under 2011. Vi har tagit del av de styrande dokument som finns upprättade internt och styr internrevisionens arbete, arbetsinstruktioner, planeringsdokument, mm.

Detaljerad bedömning av efterlevnad av IIA:s Riktlinjer

Den detaljerade bedömningen av respektive Riktlinje finns redovisad i Bilaga 1. Vid vår bedömning av efterlevnad av IIA:s Riktlinjer har vi använt oss av en bedömningsskala:

- Uppfyller IIA:s Riktlinjer
- Utrymme för förbättringsåtgärder
- Uppfyller ej IIA:s Riktlinjer.

I de fall vi har använt oss av omdömet ”Utrymme för förbättringsåtgärder” uppfyller, enligt vår bedömning, internrevisionen IIA:s Riktlinjer till huvudsakligen väsentliga delar med undantag för vissa kriterier. Granskningen har genomförts utifrån Riktlinjer för yrkesmässigt utförande av internrevision samt Yrkesetisk kod utgivna av the Institute of Internal Auditors 1 januari 2011. Vidare har vi använt oss av de bedömningskriterier som finns uppsatta av the Institute of Internal Auditors i Quality Assessment Manual, 6th edition, utgiven 2009.

Bedömning har gjorts per huvudområde. Varje huvudområde är indelat i undergrupper beskrivande viktiga attribut som ska bedömas var för sig. I de fall vi bedömt att en undergrupp inte uppfyller Riktlinjerna eller att utrymme finns för förbättring, så har detta ”dragit ned” betyget för huvudområdet. Flera huvudområden har därmed bedömts i nivå ”Utrymme för förbättringsåtgärder” trots att flera undergrupper har bedömts uppfylla Riktlinjerna.

Bedömningsskalan för bedömning av efterlevnad av IIA:s Riktlinjer finns utförligt dokumenterad i Bilaga 3.

Iakttagelser och observationer

Vi har i samband med intervjuer fått intryck av att internrevisionen uppfattas som kompetent och professionell. Medarbetarna har fått vitsord som visar på organisationens uppskattning av det engagemang och intresse för verksamheten som visas.

Sammanfattande bedömning av efterlevnad av IIA:s Riktlinjer för yrkesmässigt utövande av internrevision.

Vid en samlad bedömning av efterlevnaden mot IIA:s Riktlinjer för yrkesmässigt utövande av internrevision anser vi att Riksbankens internrevision och dess arbetssätt står i överensstämmelse med IIA:s Riktlinjer. Dock finns delområden där Riksbankens internrevision uppvisar utrymme till förbättring. Samtliga rekommendationer redovisas i Bilaga 1. Nedan följer de rekommendationer vi bedömer som väsentligast.

Igenkännandet i instruktionen av Definition av internrevision, Yrkesetisk kod och Riktlinjerna (1010)

Vi rekommenderar att när Policyn revideras med avseende på syfte, befogenheter och ansvar bör även beaktas att det ska gå att härleda Definitionen för internrevision, den Yrkesetiska koden samt Riktlinjerna.

Tillbörlig professionell omsorg (1220)

Utveckla en tydligare struktur för att gradera iakttagelser och på så sätt kommunicera till ledningen avseende kritiska områden. Detta kommer att öka förståelsen för ett kostnad-nytto synsätt i organisationen i arbetet med att reducera risker.

Leda internrevisionsverksamheten (2000)

Vi rekommenderar internrevisionen att ta fram en uppföljningsprocess för att mäta värdet som tillförs organisationen.

Leda internrevisionsverksamheten/Resurshantering (2030)

En resursanalys bör komplettera revisionsplanen där det bl.a. framgår hur tillgängliga resurser både vad avser tid och kompetens är avsedda att användas för planerade granskningar.

Arbetets beskaffenhet/Ledning (2110)

Vi rekommenderar att IR i större grad beaktar effektiviteten i organisationens etikrelaterade mål, program och aktiviteter i sin riskanalys. Vägledning vad avser tillvägagångssätt finns i Practice Advisory 2110-2 och 2110-3.

Vi rekommenderar att IR i större grad beaktar även styrningen av organisationens informations-teknologi i sin riskanalys.

Planering av uppdrag/Planeringsöverväganden (2201)

Vid upprättandet av Planerings-PM bör den inledande riskanalysen dokumenteras på ett strukturerat sätt så att härledning kan ske till de i riskanalysen identifierade riskerna.

Planering av uppdrag/Mål för uppdraget (2210)

I förstudien och/eller i uppdragsbeskrivningen ska framgå hur de risker som identifierades i riskanalysen är kopplade till målen för granskningen.

IR ska dokumentera den preliminära bedömningen av riskerna.

Vid upprättandet av planeringsdokument ska det framgå att IR genomfört en analys av sannolikheten för väsentliga fel, oegentligheter, icke-efterlevnad och annan exponering.

IR ska redovisa bedömningsgrunder för sin granskning.

Rapportera resultat/Kriterier för rapportering (2410)

Vi rekommenderar att IR definierar vad de olika graderingarna av det översiktliga omdömet står för och detta bör kommuniceras ut i organisationen.

Rapportera resultat/Rapporteringens kvalitet (2420)

Internrevisionen använder sig av en rapporteringsform som kan beskrivas som avvikelserapportering. Vi rekommenderar därför IR att i sina rapporter beskriver granskningens mål och omfattning så att det är tydligt för läsaren vad som granskats.

SAMMANFATTANDE BEDÖMNING				
IIA:s Riktlinjer för yrkesmässigt utövande av internrevision		**GC**	**PC**	**DNC**
RIKTLINJER FÖR EGENSKAPER				
1000	**Syfte, befogenhet och ansvar**		X	
1010	Igenkännandet i instruktionen av Definition av internrevision, Yrkesetisk Kod och Riktlinjerna		X	
1100	**Oberoende och objektivitet**	X		
1110	Organisatoriskt oberoende	X		
1111	Direkt samverkan med styrelsen	X		
1120	Individuell objektivitet	X		
1130	Begränsning av oberoende eller objektivitet	X		
1200	**Kompetens och vederbörlig yrkesskicklighet**	X		
1210	Kompetens	X		
1220	Tillbörlig professionell omsorg		X	
1230	Fortlöpande professionell utveckling	X		
1300	**Kvalitetssäkrings- och kvalitetsförbättringsprogram**		X	
1310	Krav på kvalitetssäkrings- och kvalitetsförbättringsprogram		X	
1311	Interna bedömningar	X		
1312	Externa bedömningar	X		

1320	Rapportera om kvalitetssäkrings- och kvalitetsförbättringsprogrammet		X	
1321	Användning av uttrycket ”Överensstämmer med *Internationella Riktlinjer för Yrkesmässig Internrevision”*	X		
1322	Redovisning av icke-efterlevnad	**E.T.**		
RIKTLINJER FÖR GENOMFÖRANDE				
2000	**Leda internrevisionsverksamheten**	X		
2010	Planering	X		
2020	Kommunikation och godkännande	X		
2030	Resurshantering		X	
2040	Principer och rutiner	X		
2050	Samordning		X	
2060	Rapportering till ledning och styrelse	X		
2070	Externa tjänsteleverantörer och organisatoriskt ansvar för internrevision	**E.T.**		
2100	**Arbetets beskaffenhet**	X		
2110	Ledning	X		
2120	Riskhantering	X		
2130	Styrning och kontroll	X		
2200	**Planering av uppdrag**		X	
2201	Planeringsöverväganden		X	
2210	Målsättning för uppdraget		X	

2220	Uppdragets omfattning		X	
2230	Resursallokering för uppdraget	X		
2240	Arbetsprogram för uppdraget	X		
2300	**Genomföra uppdrag**	X		
2310	Identifiera information	X		
2320	Analys och utvärdering	X		
2330	Dokumentera information	X		
2340	Övervakning av åtagandet	X		
2400	**Rapportera resultat**	X		
2410	Kriterier för rapportering	X		
2420	Rapporteringens kvalitet		X	
2421	Fel och utelämnanden	E.T.		
2430	Användning av ”*Utfört i överensstämmelse med Internationella Riktlinjer för Yrkesmässig internrevision*”	X		
2431	Redogörelse för icke överensstämmelse med Riktlinjerna	X		
2440	Spridning av resultaten	X		
2450	Övergripande omdöme	X		
2500	**Övervaka process och resultat**	X		
2600	**Uttalande rörande ledningens riskacceptans**	X		
	IIA Yrkesetisk kod	X		

Intervjuade personer **Bilaga 2**

Stefan Ingves	Riksbankschef
Svante Öberg	Vice Riksbankschef
Mattias Persson	Avdelningschef Finansiell stabilitet
Patrick Bailey	Internrevisionschef
Sofia Sjöqvist	Internrevisor
Carolin Wigren	Internrevisor

Bilaga 3

Bedömningsskala i enlighet med the Institute of Internal Auditors (IIA)

IIA använder sig av följande bedömningsskala i sin handbok för kvalitetsgranskning, ”Quality Assessment Manual”:

GC – “Generally Conforms” means the evaluator has concluded that the relevant structures, policies, and procedures of the activity, as well as the processes by which they are applied, comply with the requirements of the individual standard or element of the Code of Ethics in all material respects. For the sections and major categories, this means that there is general conformity to a majority of the individual *Standards* or elements of the Code of Ethics, and partial conformity to the others, within the section/category. There may be significant opportunities for improvement, but these should not represent situations where the activity has not implemented the *Standards* or the Code of Ethics, is not applying them effectively, or is not achieving their stated objectives.
Vi har i föreliggande rapport tolkat denna bedömning som “Uppfyller IIA Standards/Code of Ethics”.

PC – “Partially Conforms” means the evaluator has concluded that the activity is making good-faith efforts to comply with the requirements of the individual standard or element of the Code of Ethics, section, or major category, but has fallen short of achieving some of their major objectives. These will usually represent some significant opportunities for improvement in effectively applying the *Standards* or Code of Ethics and/or achieving their objectives. Some of the deficiencies may be beyond the control of the activity and may result in recommendations to senior management or the governing authority.
Vi har i föreliggande rapport tolkat denna bedömning som ”Utrymme för förbättringsåtgärder”.

DNC – “Does Not Conform” means the evaluator has concluded that the activity is not aware of, is not making good-faith efforts to comply with, or is failing to achieve many/all of the objectives of the individual standard or element of the Code of Ethics, section, or major category,. These deficiencies will usually have a significant negative impact on the activity’s effectiveness and its potential to add value to the organization. They may also represent significant opportunities for improvement, including actions by senior management or the governing authority.
Vi har i föreliggande rapport tolkat denna bedömning som ”Uppfyller ej IIA Standards/Code of Ethics”.