Protokollsbilaga C

Direktionens protokoll 100316, § 4 f)

PM

DATUM: 2010-03-03
AVDELNING: Internrevisionsavdelningen
HANTERINGSKLASS: Öppen
HANDLÄGGARE: Patrick Bailey

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 2009-1022 -IR

Internrevisionsavdelningens årsrapport 2009

1. Sammanfattning

Internrevisionen bedömer, utifrån de granskningar som har genomförts under 2009, att riskexponeringen för Riksbankens verksamheter är medelhög. Internrevisionen har under året i sina löpande granskningar upptäckt, 4 tillfällen då det förekommit, allvarliga brister. Bristerna rapporterades omedelbart till berörd verksamhetsansvarig som i sin tur valde att rapportera händelserna som incidenter.

Banken har under 2009 i krishanteringssyfte fortsatt att genomföra extraordinära transaktioner och likviditetsåtgärder, ofta under stor tidspress. Driftsättningen av en ny teknisk plattform för betalningssystemet skedde i februari 2009 utan incidenter. Banken har under året också påbörjat att bygga en ny kontanthanteringsdepå i Broby med en investeringsram på 350 mkr. En omorganisering av riskorganisationen i banken beslutades under senare delen av året och fanns på plats 1 januari 2010.

Revisionsplanen för 2010, som fastställdes av direktionen i slutet av 2009, är bland annat inriktad på att granska bankens processor kring finansiell stabilitet, betalsystemet, valutareservförvaltningen och ny kontanthanteringsdepå i Broby.

2.1 Granskningsarbetet

Internrevisionens uppgift är att på direktionens uppdrag genomföra granskningar och avge bedömningar utifrån följande utgångspunkter:

- Efterlevnad av lagar, regler och riktlinjer
- Riskhantering
- Måluppfyllelse
- Säkerställande av tillförlitlig och riktig beslutsinformation
- Skydd av tillgångar, information och värden

- Hushållning med resurser

Revisionsarbetet har följt prioriteringarna i revisionsplanen utifrån riskanalysen. Revisionsresurserna har till övervägande del nyttjats till granskningar och uppföljningar. En mindre del har utnyttjats för bevakning och rådgivning. Samarbete har skett med Riksdagens revisorer och Riksrevisionen och dessa har nyttjat internrevisionens arbete för att inom vissa områden begränsa sina insatser. Under året har både nya granskningar och uppföljningar av utestående iakttagelser genomförts.

Under 2009 har 21 (15) granskningsrapporter och 19 (29) uppföljningsrapporter avlämnats. Dessa resulterade i 62 (56) nya iakttagelser och 41 (54) iakttagelser som kunde avslutas. Den utgående balansen är 79 (58) öppna iakttagelser, varav 44 (32) härrör från årets granskningar.

Under året 2009 har granskningar genomförts och revisionsrapporter avgivits inom framförallt de områden som anges nedan. Bedömning har skett av intern styrning och kontroll samt riskhantering.

2.1.1 Kärnprocesser

• Penningpolitik	Genomförande av Penningpolitik – Finjusteringar
• Betalningsväsendet	Granskning av verksamhetens drift av RIX Kontanthantering – Bankdepåer Kontanthantering – Sedelmakulering Likviditetsåtgärder Säkerhetskrav i RIX
• Tillgångsförvaltningen	Systemförvaltning av Dimension

2.1.2 Stödprocesser

• IT-stöd	Behörighetshantering – Colin och RIX Behörighetshantering – Caesar Ändringshantering i infrastruktur
• Ekonomi	Granskning av tertialbokslut Granskning av bokföring av likviditetsåtgärder
• Säkerhet	Informationssäkerhet
• Strategisk Ledning	Verksamhetsstyrning/ RYC Sourcing Implementering av ISK

- Personal — Kompetensförsörjning

Driftsättning av nya tekniska system medför ofta ökade risker för driftstörningar eller avbrott. Riskerna inom betalningsväsendet ökade under året när driftsättningen av en ny teknisk plattform för betalningssystemet skedde i februari, men störningar eller avbrott uteblev.

För en fullständig förteckning av avlämnade revisionsrapporter under året 2009, se bilaga 1.

2.2 Incidenter under pågående granskningar

Internrevision har under årets löpande granskningar upptäckt, vid 4 tillfällen, allvarliga brister som vi omedelbart rapporterade till berörd ledning, som i sin tur valde att rapportera händelser som incidenter ofta innan våra granskningar var slutförda. Följande granskningar berördes:

Betalningsväsendet	– Granskning av likviditetsstöd till Kaupthing Sverige AB.
	– Säkerhetskrav i RIX.
Kontanthantering	
	– Sedelmakulering (Tumba) .
Tillgångsförvaltning	
	– Systemförvaltning av Dimension.

2.3 Rådgivning

Rådgivning har främst skett inom områdena:

Betalningsväsendet	
	Deltagit som observatör i FRIX styrgrupp.
	Deltagit i rådgivningsmöte när det gäller åtgärdsarbetet med öppna iakttagelser inom betalningsväsendet.
	Utbildning – Introduktion i RIX. Syftet var först att sätta ihop en utbildning för nyanställda internrevisorer. Intresset växte så att det till slut var medarbetare från olika avdelningar som deltog.
Riskhantering	
	Deltagit som observatör i ISK implementerings styrgrupp.

2.4 Internationella uppdrag

Internrevisionen har varit aktiva inom:

- ESCB som medlem i Internal Auditors Committee.
- G10 på chefsnivå och i en grupp för IT-revisorer. Arbetat i en arbetsgrupp med temat Continuous Auditing.
- Ett samarbetsforum för Nordiska centralbankers internrevisionschefer, som Sveriges Riksbank kommer att vara värd för under 2010.
- Internrevisionschefen bjöds in som talare vid Central Banking Publications seminar- "Effective Internal Audit for Central Banks".

3. Resurser, kvalitets-, metod- och kompetensutveckling

Internrevisionsavdelningen hade en budgetram på 5 åa, men det faktiska utfallet under 2009 blev 4,5 åa. Det beroende på att en tjänst var vakant fram till maj 2009 och en tjänst bestod i en deltid föräldraledighet. Externa konsulter har upphandlats för 3 (1) co-sourcing granskningar under året.

Internrevisionens arbete har bedrivits i enlighet med god sed för internrevision, vilket innebär att arbetet har bedrivits i överensstämmelse med The Institute of Internal Auditors (IIA) Standards och IIA:s Code of Ethics. I början av 2006 genomgick internrevisionsverksamheten en extern kvalitetsutvärdering. Under 2007 gjordes en intern kvalitetssäkring. Resultatet av utvärderingarna visar att verksamheten bedrivs i enlighet med god sed för internrevision.

Alla som arbetar på internrevisionsavdelningen är medlemmar i The Institute of Internal Auditors.

Inom Sverige deltar vi i nätverk inom the Information Systems Audit and Control Association (ISACA) och Internrevisorernas förening för att hålla oss uppdaterade och sprida information om vår verksamhet.

4. KIRR

Internrevision har under året initierat en ny process med en rapport, Konsoliderade Internrevisions Rapport (KIRR), där man konsoliderar alla öppna revisionsiakttagelser i banken. Syfte med processen är följande:

– att ge avdelningschefer en samlad bild och status av sina öppna revisionsiakttagelser

– att verksamheten bättre kan planera och löpande följa upp åtgärdsarbetet

– att skapa en bättre dialog mellan internrevisorer och avdelningar, och också mellan avdelningar, om möjliga problem eller hinder för ett lyckat åtgärdsarbete samt

– att avdelningsvis samla in information om förändringen i åtgärdsstatus för att effektivisera internrevisionens uppföljningsprocess samt stå till förfogande för stöd och råd kring det löpande åtgärdsarbetet.

För att processen ska ge ett värde för både verksamheten och internrevision krävs att vi får kompletta svar från samtliga avdelningar. Alla avdelningar har inte svarat på utskicket eller lämnat kompletta svar som innebär att materialet är av mindre värde och syfte med processen fallerar. Internrevision ska under 2010 ta ställning till om vi ska fortsätta med processen.

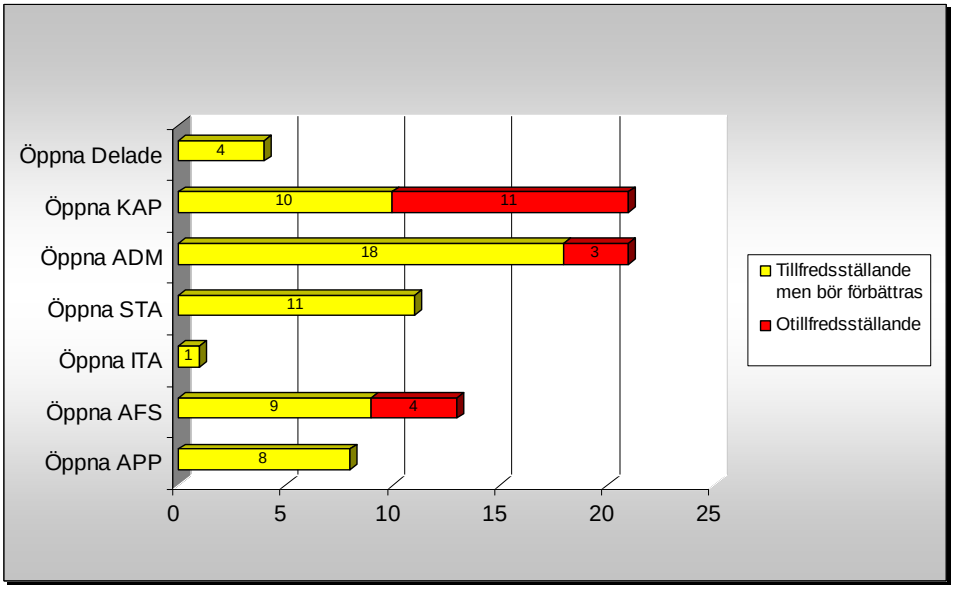
5.1 Verksamhetens hantering av öppna internrevisionsiakttagelser

Vi har under året analyserat verksamhetens hantering av öppna revisionsiakttagelser. Vi har noterat att många iakttagelser inte stängs inom den tid som verksamhet har satt i sitt svar till internrevisionen. Analysen visade att majoritet av de öppna revisionsiakttagelserna åtgärdas inte i tid. Dessutom visade analysen att det krävs flertal uppföljningar från internrevisionen innan iakttagelser åtgärdas.

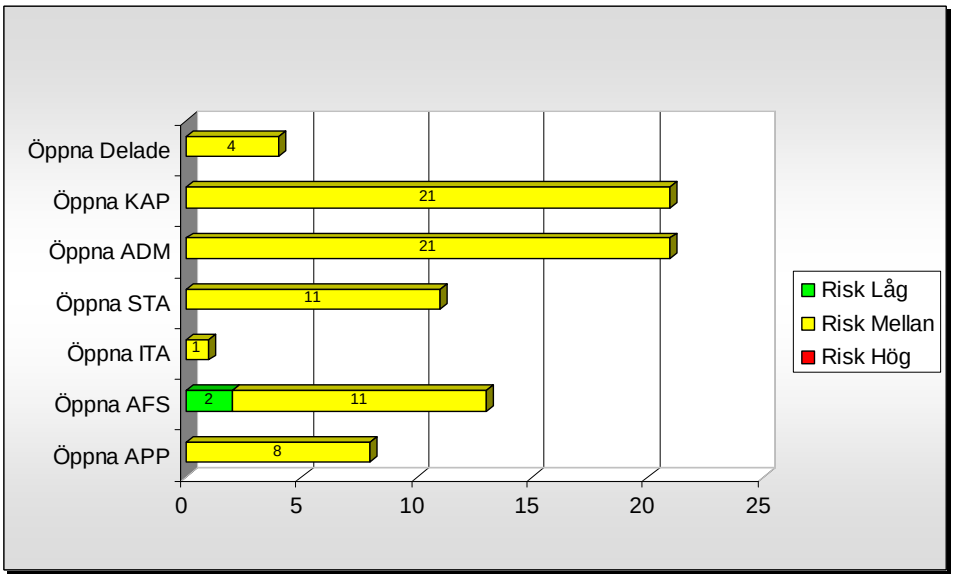
När verksamheten inte genomför överenskomna åtgärder inom överenskommen tid måste vi internrevisorer genomföra flera uppföljningar av samma revisionsrapport, vilket medför ineffektivitet både i avdelningens arbete och i vårt revisionsarbete.

5.2 Öppna iakttagelser

Det fanns 79 öppna revisionsiakttagelser vid årets slut varav 18 hade revisionsbedömning otillfredsställande och 61 revisionsbedömning tillfredställande men bör förbättras (Fig. 1). Inga öppna revisionsiakttagelser vid årets slut bedöms i nuläget som hög risk. Alla iakttagelser bedöms ha en risknivå mellan, med undantag för 2 som bedöms som låg (Fig. 2).



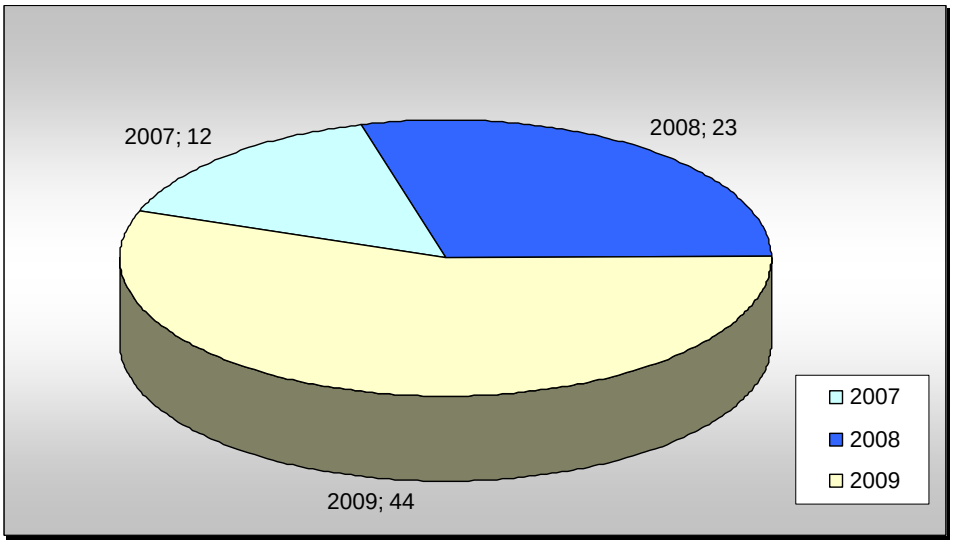
Figur 1: Öppna revisionsiakttagelser per avdelning – Revisionsbedömning per 31-12-2009



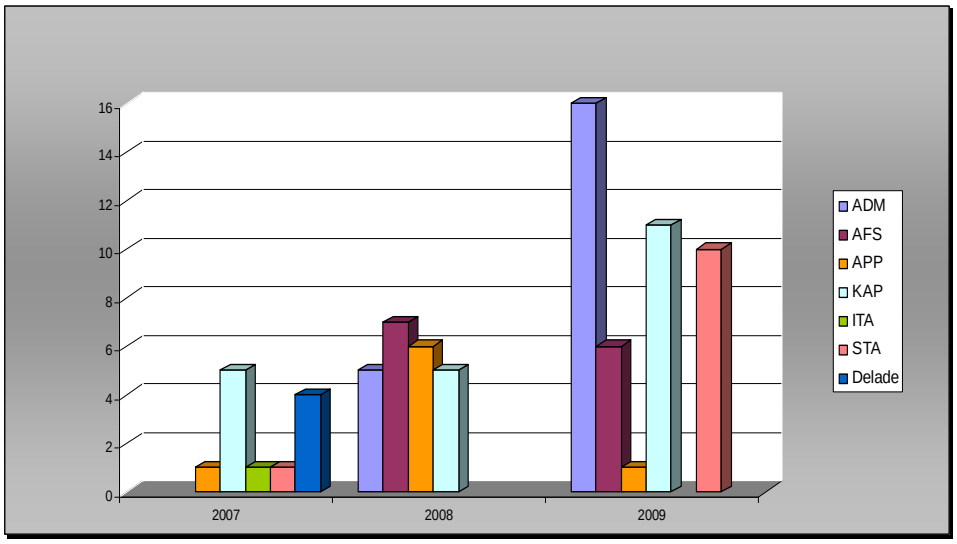
Figur 2: Öppna revisionsiakttagelser per avdelning – Riskbedömning per 31-12-2009

5.2 Åldersfördelning av öppna iakttagelser

Verksamheten har under året åtgärdat 41 (54) revisionsiakttagelser bl.a. äldre iakttagelser från 2004-2006. Kvarstående öppna iakttagelser vid årsskiftet är från åren 2007-2009 med fördelning enligt Figur 3 och 4.



Figur 3: Åldersfördelning av öppna revisionsiakttagelser per 31-12-2009



Figur 4: Åldersfördelning av öppna revisionsiakttagelser (avdelningar) per 31-12-2009

6. Samarbete med Finansinspektionen

Under december 2009 har internrevision inlett ett samarbete med Finansinspektionen för att leverera internrevisionstjänster. Överenskommelsen löper på 3 år och ska utvärderas efter 18 månader.

Bilaga 1: Förteckning över avlämnade revisionsrapporter

Dnr	*Typ av ärende*	*Namn på dokumentet*
2009-0035-IR	Uppföljning	BV, Betalningsavveckling
2009-0186-IR	Granskning	BV, Övervakning och finansiell analys, CNG
2009-0205-IR	Uppföljning	VF, roller och ansvar KAP
2009-0228-IR	Uppföljning	EK, Applikationsgranskning Agresso
2009-0239-IR	Granskning	SL, Sourcing.doc
2009-0345- IR	Granskning	BV, SEK utlåning mot säkerhet i företagscertifikat
2009-0346-IR	Granskning	BV, US-dollar utlåning
2009-0354-IR	Uppföljning	VF, roller och ansvar AFS
2009-0407-IR	Granskning	IT, Ändringshantering
2009-0434-IR	Uppföljning	SÄK Övergripande säkerhet
2009-0455-IR	Uppföljning	VF, roller och ansvar KAP
2009-0526-IR	Uppföljning	BV, Makulering Tumba
2009-0607-IR	Uppföljning	PP, Implementation
2009-0654-IR	Granskning	BV, Övervakning och finansiell analys, KPTH
2009-0661-IR	Granskning	SÄK, Informationssäkerhet INF
2009-0661-IR	Granskning	SÄK, Informationssäkerhet SÄK
2009-0662-IR	Granskning	IT, Behörighetshantering Colin och Rix
2009-0663-IR	Granskning	IT, Behörighetshantering Caesar
2009-0708-IR	Uppföljning	IT Projekt SAM 2b
2009-0714-IR	Granskning	BV, Inventering av depåer
2009-0746-IR	Granskning	SL, Verksamhetsstyrning

2009-0757-IR	Uppföljning	BV, Anskaffning sedlar
2009-0761-IR	Uppföljning	BV, Makulering
2009-0820-IR	Granskning	BV, Säkerhetskrav RIX
2009-0831-IR	Uppföljning	BV, Kontanthantering depåer
2009-0874-IR	Uppföljning	IT, Behörighetshantering Colin RIX
2009-0883-IR	Uppföljning	PP, Prognosprocessen
2009-0896-IR	Granskning	SL, Implementering av intern styrning och kontroll ramverk
2009-0926-IR	Granskning,	EK, Teritalbokslut
2009-0927-IR	Granskning	EK, Bokföring av likviditetsåtgärder
2009-0937-IR	Granskning	BV, Drift och förvaltning av Rix
2009-0946-IR	Uppföljning	BV, Inlösen sedlar
2009-0947-IR	Uppföljning	VF, Riskmätning likviditetsrisk
2009-0997-IR	Uppföljning	BV, Övervakning och finansiell analys, CNG
2009-0998-IR	Granskning	PP, Finjusteringar
2009-1001-IR	Uppföljning	EK, Tertialbokslut
2009-1002-IR	Uppföljning	BV, Övervakning och finansiell analys, KPTH
2009-1003-IR	Granskning	VF, Systemförvaltning Dimension
2009-713- IR	Granskning	BV, Sedelmakulering
2009-1017- IR	Granskning	SL, Kompetensförsörjning