Protokollsbilaga C
Direktionens protokoll 2017-12-14 § 5

Beslutsunderlag

DATUM: 2017-12-08
AVDELNING: Internrevision
HANDLÄGGARE: Simon Rörborn

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 [Diarienummer]

Revisionsplan 2018

Förslag till direktionens beslut

Direktionen fastställer revisionsplanen för år 2018 i enlighet med vad som anges i detta beslutsunderlag. Direktionen fastställer även med vilken lägsta periodicitet väsentliga områden ska beröras av en granskning.

Bakgrund

Revisionsplanen för 2018 omfattar beskrivning av och prioriteringar för internrevisionsavdelningens (IR) revisionsverksamhet. Beslut om resurstilldelning och övergripande verksamhetsinriktning för IR fattas av direktionen. För de granskningar som berör europeiska centralbankssystemet, ESCB, fattas beslut av ECB-rådet.

Sammanfattningsvis fortsätter IR sin process- och riskbaserade revisionsansats där metoderna löpande fördjupas och vidareutvecklas. Genom denna ansats får IR en målorienterad syn på Riksbankens arbete som gör det möjligt att upprätthålla en helhetssyn.

Riksbankens verksamhet granskas av internrevisionen, fullmäktiges revisorer och Riksrevisionen. Internrevisionen ska samarbeta med övriga granskningsorgan för att höja kvaliteten och effektiviteten på granskningarna.

Överväganden

De prioriterade granskningar som ska genomföras under 2018 presenteras löpande under avsnitt två. Under avsnitt tre presenteras ytterligare granskningar som tas med i planen i mån av tid. Dessa granskningar är listade i en prioriteringsordning.

Riskbedömning

Revisionsplanen grundar sig på prioriteringar av de områden där IR bedömer att brister i den interna styrningen och kontrollen får störst påverkan på verksamheten.

De områden inom Riksbankens verksamhet som är av avgörande betydelse för måluppfyllelse bör granskas kontinuerligt, medan övriga områden generellt inte behöver uppmärksammas med samma frekvens.

Riskbedömningen bygger på en genomgång av bankens övergripande riskanalys och verksamhetens egna riskanalyser, självutvärderingar, inrapporterade incidenter av väsentlig karaktär samt bankens strategiska prioriteringar.

Nedan följer ett utkast för den periodicitet med vilken respektive område minst bör revideras. Eventuella avvikelser mot detta ska presenteras i förslaget till revisionsplan.

OMRÅDE	**PERIODICITET**
IT	1 år
Ledningsprocessen	1 år
Inventering	2 år
Kontanthantering	2 år
Outsourcad verksamhet	3 år
Projekt	3 år
Inköp	3 år
Kontinuitet	3 år
Guldinnehav	5 år
Fysisk säkerhet	5 år

Granskningar

Nedan följer de föreslagna granskningarna. Granskning 1-11 bedöms kunna genomföras under året. Granskningarna 12- genomförs i mån av tid. Planen kan när som helst justeras genom nytt beslut av direktionen.

Granskningar inom planen

	Rubrik	**Preliminär beskrivning**
1	Cybersäkerhet och SWIFT	Den första delen av granskningen är initierad av ECB och är därmed obligatorisk för oss. Den andra delen bygger på vårt avtal med SWIFT som eventuellt kommer innebära en viss granskning från vår sida.
2	Fristående guldinventering	I enlighet med Internrevisions policy skall vi regelbundet, minst vart 5 år, inspektera alla våra guldinnehav i utlandet. Under 2018 skall vi göra en inspektion.
3	Strategi- och VP-processen	Processen från att utveckla en strategi till att få den levande i organisationen är avgörande för ett effektivt arbete. I denna granskning fokuseras på hur väl processen och därmed strategin är förankrad i organisationen.
4	Styrande dokument / Försvarslinjerna	En väsentlig styrmekanism inom Riksbanken utgörs av våra policyer, regler och handböcker. I denna granskning reviderar vi hur intern styrning och kontroll avseende rutiner och struktur för dessa styrdokument fungerar. Vi granskar även hur våra försvarslinjer arbetar med dessa styrdokument.
5	Projektmodellen	Inom Riksbanken genomförs årligen en stor mängd projekt. Styrning av projekten i förhållande till en väl avvägd projektmodell kan vara avgörande för framdrift och effektivitet i dessa projekt. Vi granskar intern styrning och kontroll i styrning av våra signifikanta projekt.
6	Lagerhantering / Makulering – Kontanter	Kontanthanteringen inom Riksbanken har förändrats under de senaste åren. Rutiner och arbetssätt har historiskt visat sig ha brister. Rutinerna har under 2017 justerats. Vår granskning fokuserar på de nya arbetssätten och att den interna styrningen och kontrollen nu är effektiv och ändamålsenlig.
7	Programförändringar	Vår verksamhet är mycket beroende att väl fungerande IT-stöd. En nyckel för fortlöpande säker och stabil IT-drift är väl fungerande rutiner för programförändringar. Granskning följer processen från utveckling via test till implementering av ny kod i vår driftmiljö.
8	Handel med värden	Riksbanken handlar på marknaden för stora värden. Handelsprocessen är därför en nyckelprocess. Vår granskning fokuserar på signifikanta kontroller i processen för att säkerställa

		god intern styrning och kontroll. Vi kommer t.ex. granska hantering av limiter och handelsbeslut.
9	Logisk behörighet	Behörighet till vår IT-miljö och därmed vår information är en grundförutsättning för väl fungerande Information- och IT-säkerhet. Granskningen fokuserar på tilldelning, periodisk verifiering samt borttag av behörigheter, d.v.s. för hela cykeln för behörighetsadministration.
10	Förvaltningsmodellen	Under den senaste perioden har vi inom Riksbanken infört en ny modell för förvaltning av vårt IT-stöd. Modellen har bl.a. uppdaterats för att öka effektiviteten i vår förvaltning och tydliggöra ansvaret för vårt IT-stöd. Granskningen fokuserar på designen av den nya modellen samt implementering av det nya arbetssättet.
11	Inlösenprocessen	Riksbanken löser in sedlar som är obrukbara. De kan t.ex. röra sig om gamla sedlar. Antalet ärenden i inlösen har i.o.m. sedelutbytet varit högt de senaste åren. Granskningen fokuserar på processens senare delar, d.v.s. lagerhantering och avslut.

Granskningar i mån av tid

	Rubrik
12	IT Asset Management
13	Styrning av molntjänster
14	Transaktioner i RIX
15	Personuppgifter – GDPR
16	Fysisk säkerhet – värden
17	Back-up
18	Nytt lönesystem
19	HR
20	Internationellt arbete
21	Forskning
22	Attester
23	Outsourcing

Resurser

De granskningar som föreslås för 2018 genomförs i huvudsak med interna resurser inom IR. Avdelningen har en ram på 5 årsarbetare. Externa konsulter kan avropas för att biträda vid de planerade granskningarna.