Protokollsbilaga B
Direktionens protokoll 2020-09-15 §5

Beslutsunderlag

DATUM:	2020-09-15
AVDELNING:	Internrevision
HANDLÄGGARE:	Simon Rörborn
HANTERINGSKLASS	Ö P P E N

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 2020-00905

Förändring av tidigare fastställd revisionsplan

Förslag till direktionens beslut

Direktionen beslutar att ändra tidigare beslutad revisionsplan för Internrevision 2020, diarienummer 2019-01320, enlig följande:

- Granskning 20001 IT systems in operation utgår, om ESCB så beslutar, samt att en ny granskning av IT network & telecommunication infrastructure in operation utförs, om ESCB så beslutar.
- Granskning 20002 Inventering utgår
- Granskning 20010 GDPR utgår
- Ny granskning av HR-områdena avseende rekrytering samt ”Organisatorisk och social (psykosocial) arbetsmiljö”

Ärendet

20001 IT Systems in operation samt IT network & telecommunication infrastructure in operation

Den beslutade granskningen 20001 ”IT systems in operation” är en av ESCB bestämd granskning. Till följd av en riskanalys av Internal Auditors Committée inom ESCB förslås att denna skjuts upp till nästa år och en granskning av ”IT network & telecommunication infrastructure in operation” utförs istället. Ett förslag till beslut ligger hos ESCB och beslut väntas inom kort.

20002 Inventering

Enligt Riksbankens policy för internrevision bör våra innehav i utländska gulddepåer inspekteras minst vart femte år. Under 2018 lades en inventeringsplan som initialt utökade denna period till sju år. Under 2020 var planen att besöka en av våra depåer för inventering. Coronapandemin har dock inneburit att det är mycket svårt att genomföra en inventering under hösten 2020. Detta pga omfattande besöks- och reserestriktioner kombinerat med hög arbetsbelastning i berörd avdelning inom Riksbanken. Därför föreslår jag att den beslutade granskningen stryks från revisionsplanen 2020. Detta skulle även innebära att den initiala inspektionsperioden förlängs från sju till åtta år.

20010 GDPR

Revisionsplanen för 2020 inkluderade en granskning av intern styrning och kontroll avseende Riksbankens hantering av personuppgifter samt efterlevnad av dataskyddsförordningen.

Bakgrund

Inför införande av GDPR tillsattes en arbetsgrupp, tillsammans med en extern projektledare, för att arbeta med Riksbankens interna GDPR förberedelser i syfte att etablera ett grundläggare arbete med dataskydd. Projektet avslutades i juni 2018 och den övergripande slutsatsen var att Riksbanken bedömdes vara väl förberedd inför GDPR per den 25 maj 2018.

Nuvarande status

Revisionsbolaget Deloitte är numera Riksbankens externa dataskyddsombud (DSO) och är organisatoriskt placerad på STA/RIE. Ett dataskyddsombuds huvudsakliga arbetsuppgift är att kontrollera och övervaka att organisationen följer dataskyddsförordningen (GDPR) genom insatser och aktiviteter. Vidare kommer DSO stötta och informera verksamheten i dataskyddsfrågor samt ge vägledning kring dataskyddsarbetet på banken.

En övergripande gap-analys har genomförts med syfte att utvärdera Riksbankens implementation och arbete avseende GDPR. Baserat på analysen kommer en åtgärdsplan arbetas fram där åtgärderna specificerar vilka åtgärder Riksbanken behöver genomföra för att åtgärda noterade gap samt öka sin mognadsgrad. Planen kommer även inkludera åtgärder definierade i de tidigare dataskyddsplanerna för 2019 och 2020. Insatserna kommer kräva tid och resurser från verksamheten. Tidplanen för implementering är därför i dagsläget osäker men DSO beräknar att Riksbanken höjer sin mognadsgrad per 31/12 2020.

Slutsats

Internrevisionens granskning skulle med stor sannolikhet notera de områden som redan identifierats genom den gap-analys som genomförts. Internrevisionens bedömning är därför att vår insats skulle leda till hög belastning samt ”onödig” stress i verksamheten samt ineffektivitet i användningen av de granskande resurserna i organisationen. Jag föreslår därför att granskningen av GDPR stryks från Internrevisionsplanen 2020.

HR processer

Rekryteringsprocessen är en av de grundläggande processerna för att organisationen ska fungera på ett tillfredsställande sätt. Som myndighet krävs det att vi även har en mycket transparant och tydlig process för att säkerställa att vi får in den bästa kandidaten för uppdraget och samtidigt följa de lagar och regler som är styrande på området. Under hösten 2020 finns ett ärende i personalansvarsnämnden rörande rekryteringsprocessen.

Vidare har Riksbanken som arbetsgivare ett stort ansvar vad avser den organisatorisk och social (psykosocial) arbetsmiljön för alla våra medarbetare. I samband med den pågående pandemin uppstår nya utmaningar inom området. Vår förmåga att möta dessa utmaningar är beroende av en väl fungerande struktur för intern styrning och kontroll inom detta område.

Med anledning av att dessa områden är av stor vikt för Riksbanken som organisation föreslår jag en ny granskning in HR med fokus på dessa två områden.

Sammanfattning

De föreslagna förändringana i Internrevisionsavdelningens revisionsplan innebär att den totala planen ser ut som följer:

Nr	Ämne	
20001	IT systems in operation (ESCB)	Struken
20002	Inventering	Struken
20003	Kontanthantering	
20004	Styrning av utlagd verksamhet	
20005	IT-generella kontroller RIX inkl. kontinuitet	
20006	Intern styrning och kontroll på enhetsnivå	
20007	Molntjänster	
20008	Logiska behörigheter	
20009	Styrning av cybersäkerhet	
20010	GDPR	Struken
20011	Dok. av direktionsbeslut i samband med Coronapandemin	Tillagd T2
20012	IT network & telecommunication infrastructure in operation (ESCB)	Tillagd T3
20013	HR-områdena rekrytering och arbetsmiljö	Tillagd T3