Protokollsbilaga F1
Direktionens protokoll 2019-12-12 §8

Utkast Revisionsplan IR 2020

2019-12-03

SVERIGES RIKSBANK

Introduktion

Internrevisionsavdelningen har under hösten genomfört ett arbete för att identifiera potentiella revisionsområden. Vi har bl.a. intervjuat direktionen, avdelningschefer och Riksbanksfullmäktiges ordförande och vice ordförande samt tagit del av riskanalyser, verksamhetsplaner och omvärldsanalyser. Utifrån en totallist har vi prioriterat revisionsområdena. Vår bedömning är att 10 revisioner bör genomföras under 2020.

Revisionsplan innehåller m.a.o. de 10 mest väsentliga revisionsområdena. I detta material finns även ett antal potentiella revisionsområden medtagna som inte kom med i revisionsplanen.

Utkastet till revisionsplan presenterades för Direktionen den 2 december och framläggs för beslut den 12 december.

Översikt - Revisionsplan 2020

	Rubrik	STA	AFB	APP	AFM	AVS	AFS
1	IT Systems in operation (ESCB)					✓	
2	Inventering				✓		
3	Kontanthantering		✓				
4	Styrning av utlagd verksamhet	x				✓	
5	IT-generella kontroller RIX inkl. kontinuitet		✓			x	
6	Intern styrning och kontroll på enhetsnivå	✓	x	x	x	x	x
7	Molntjänster	x	x	x	x	✓	x
8	Logiska behörigheter	x	x	x	x	✓	x
9	Styrning av cybersäkerhet	✓				x	(x)
10	GDPR	✓	x	x	x	x	x

✓ Sponsor i LG
x Avdelning som även berörs av granskningen

Revisionsplan 2020

	Rubrik	Preliminär beskrivning
1	IT Systems in operation (ESCB)	En granskning fastställd i ESCB och därmed obligatorisk för oss.
2	Inventering	I enlighet med Internrevisions policy bör Internrevision regelbundet, minst vart 5 år, inspektera alla våra guldinnehav i utlandet. Under 2020 bör en depå inspekteras.
3	Kontanthantering	Kontanthantering är en väsentlig del av Riksbankens uppdrag och verksamhet. Området innehåller inneboende risker som hanteras genom en befintlig kontrollstruktur. Senaste granskningen av området genomfördes 2018. Vår granskning fokuserar på intern styrning och kontroll inom nuvarande arbetsprocesser för bl.a. lagerhantering och makulering.
4	Styrning av utlagd verksamhet	Intern styrning och kontroll över våra väsentliga processer är en grund för god myndighetsstyrning. Detta gäller även verksamhet som vi valt att utföra med hjälp av annan part, sk utlagd verksamhet (outsourcing).

Revisionsplan 2020

	Rubrik	Preliminär beskrivning
5	IT-generella kontroller RIX inkl. kontinuitet	RIX är ett av våra mest väsentliga system. En säker och robust hantering av IT-generella kontroller krävs för att systemet ska fungera ändamålsenligt. Inom denna granskning fokuserar vi på behörigheter, programförändringar och hantering av kontinuitet.
6	Intern styrning och kontroll på enhetsnivå	Granskningen fokuserar på att den interna styrningen och kontrollen på enhetsnivå följer den övergripande strukturen som gäller för Riksbanken.
7	Molntjänster	Användning av molntjänster förväntas öka under de kommande åren. Granskning av intern styrning och kontroll inom området och kommer att omfatta kartläggning och livscykelanalys av Riksbankens rutiner och beredskap för användning av molntjänster.

Revisionsplan 2020

	Rubrik	Preliminär beskrivning
8	Logiska behörigheter	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.
9	Styrning av cybersäkerhet	Cybersäkerhet är ett strategisk viktigt område för Riksbanken och området har varit under stark förändring de senaste åren. Granskningen fokuserar på att vi har en god och väl fungerande struktur för styrning och kontroll.
10	GDPR	Inom Riksbanken hanterar vi stora mängder data. En viss del av denna data utgörs av personuppgifter. Hanteringen av denna typ av data är reglerad genom Dataskyddsförordningen. Vår granskning fokuserar på intern styrning och kontroll avseende Riksbankens hantering av personuppgifter samt efterlevnad av dataskyddsförordningen.

Andra tänkbara revisionsområden

Område
Krisberedskap
Licenshantering
Programförändringar
Hållbarhet
RIX transaktionsflöden
Finansiella risker
Kommunikationsprocesserna
Leverantörsstyrning
ISK processen
Dimension
QCMS
Jäv

Fastställd minsta periodicitet för väsentliga revisionsområden*

OMRÅDE	PERIODICITET	Senast	Plan 2020
Ledningsprocessen	1 år	2019	6, 9
RIX	1 år	2019	4, 5, 9
IT	1 år	2019	4, 5, 7, 8
Inventering	2 år	2018	3
Kontanthantering	2 år	2018	3
Outsourcad verksamhet	2 år	2018	4, 5, 8
Projektprocessen	3 år	2019	-
Inköp	3 år	2019	-
Kontinuitet	3 år	2017	3, 5
Guldinnehav	5 år**	2019	2
Fysisk säkerhet	5 år	2019	-

* Minsta periodicitet enl Riksbankens policy för internrevision
** Tillfällig förlängning till 7 år – tom 2021

Övriga löpande / större arbeten inom IR under 2020

IR planerar även att deltar som adjungerad i följande fora

1. ISK-kommittén
2. IT- och Digitaliseringskommittén
3. Kommittén för IT-säkerhetsfrågor (Cyberkommittén)
4. Utvalda projekt – ev eKrona, Transition, TFÖ

Övrigt

1. ESCB – Internal Audit Committee
2. BIS - CBIA – Internal Audit developement