PM Beredning av väsentliga verksamhetsförändringar

Bilaga 2

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 2022-00417

DATUM:	2022-03-30
AVDELNING:	Stabsavdelningen
HANDLÄGGARE:	Pether Burvall
HANTERINGSKLASS	Ö P P E N

Omorganisering styrning informationssäkerhet

Mallen används vid beredning av väsentliga verksamhetsförändringar.

En riskanalys har genomförts för ett förslag som i korthet innebär en överflyttning av nuvarande CISO-roll från STA/RIE till AVS/SÄK. AVS/SÄK får därmed ansvar för kravställande av säkerhet i alla perspektiv, inklusive informationssäkerhet. STA/RIE fokuserar i och med det på en mer renodlad andra linjen-roll. Förslaget ingår i en prioriterad utveckling av Riksbankens cyber-/informationssäkerhet som även innefattar relativt kraftiga resursförstärkningar för såväl kravställande SÄK, som för AID som fortsatt ansvarar för att hitta lösningar och leverera på kraven med egna resurser och köpta tjänster.

Ansvarig/Sponsor: Thomas Lundin

Projektledare: Pether Burvall

Koordinator: Pether Burvall

1. Intressenter

- Riskenheten (obligatorisk) Deltagare: Rickard Faleij, Jeanette Kronwall. Dessutom har riskchef Mia Holmfeldt har lämnat synpunkter via mail.
- Säkerhetsenheten (obligatorisk) Deltagare: Thomas Lundin, Daniel Saretok
- IT (obligatorisk) Deltagare: Sinisa Cicovic, Anna-Carin Joelsson
- Rättssekretariatet (obligatorisk) Deltagare: Sofie Strandberg
- Övriga intressenter AVS/HR: Emma Pelarhagen

2. Riskanalys

Namn på projekt/initiativ	Ansvarig	Samordnare	Deltagare
Omorg styrning infosäk	Thomas L, Direktionen	Pether Burvall	Thomas Lundin, Pether Burvall, Rickard Faleij, Anna-Carin Joelsson, Sinisa Cicovic, Jeanette Kronwall, Sofie Strandberg, Daniel Saretok, Emma Pelarhagen

Upplevd koncensus kring att åtgärden framför allt bör vara riskmitigerande, jmf med nuvarande org - men följande risker bör beaktas:

Beskrivning av operativa risker				Riskägare	Nettorisker			Hantering av risk		
Risk-id	Avd/ Enhet	Riskbeskrivning: *"Risk för/att..."*	Orsak till risken: *"Pga att..."*		S (1-5)	K (1-5)	Risk (L, M, H)	Åtgärd	Färdig-ställande datum	Ansvarig
1	AID, SÄK	Kravställande org för resursstark och ambitiös i förhållande till utförarens (som ska hitta lösningar och åtgärda) förutsättningar = svårarbetad styrmodell. Risk för störningar i AID:s utvecklingsspår.	SÄK ökar resursinsatsen relativt kraftigt i samband med att övertagandet av ansvaret för infosäk	Säkerhetschef	2	3	M	Stor resursförstärkning även på AID. Olika åtgärder för att skapa samsyn i bankens målbild. Planera uppstart med kickoff för samtliga roller - där mål och färdplan diskuteras gemensamt.	dec-22	Delat ansvar CISO och övr ansvarsroller
2	AID, RIE, SÄK	Vi är kvar i en mer uppdelad org trots förändringen, att samordning inte sker fullt ut.	Bristande kommunikation och otydlig rollfördelning	Säkerhetschef, Riskchef	2	3	M	Utveckla tydliga roller och ansvar - lednings- och personalinformation	maj-22	CISO/ Säk.chef
3	RIE, SÄK	Att RIE tappar information som behövs för att man ska kunna uppfylla sitt uppdrag, när avståndet ökar mellan 1a och 2a linjen - samt att antalet avstämningsytor för CISO ökar för att informera t ex RIE	Tidigare informationskanaler försvinner när CISO flyttar	Säkerhetschef, Riskchef	2	3	M	Bestämma forum och samarbetsformer som säkerställer att 2a linjen bjuds in och får ta del av relevant information ang infosäk och säkerhetsskydd - dvs. SÄK i samarbete med RIE fastställer vilka forum som RIE/2:a linjen deltar i för att få relevant information. Effektiva rapporterings-/informationskanaler för att underlätta för CISO att rapportera till 2a linjen för att bevara en god informationsdelning.	maj-22	Riskchef/ Säk.chef
4	SÄK	SÄK blir utmanande att leda och styra. Även risk för oro/osäkerhet på nuvarande SÄK, då enheten växer och en ny funktion etableras.	SÄK:s uppdrag och resurser blir så omfattande (17 tjänster)	Säkerhetschef	4	3	M	Intern översyn av SÄK:s organisation och ansvarsroller	sep-22	Säk.chef
5			Infosäk, säk.skydd är integrerat - kan inte separeras i en org.modell	Säkerhetschef	4	2	M			
6	RIE	Utvecklingen av dataskyddet kan tappa i effektivitet	Avståndet till CISO ökar, nu samlokaliserat på RIE	Dataskydds-ombudet	2	1	L	Utnyttja att vi är en liten org, relationsbyggande över enhetsgränser. Gäller inte bara Dataskydd och CISO utan även Dataskydd/AID.	Löpande	DSO och CISO
7	SÄK, AID, HR	Otydlig bild externt bland de kompetenser vi vill fånga, vilket gör att det kan bli svårt att få rätt kandidater, eller att vi konkurrerar om samma kandidater	Brist på koordinering av annonsering m m mellan SÄK o AID	AID, SÄK, HR	3	2	M	Samordning av en bankgemensam bild i annonserna (AID, SÄK, HR)	Vid rekr	AID, SÄK, HR
8	SÄK, AID	Ledningsrapportering (riskbild, status) blir bristfällig	Om endast nya SÄK ledningsrapporterar.	AID, SÄK	3	2	M	Ledningsrapportering en del av arbetet med helheten enligt risk 1. AID tar fram förslag till ledningsrapportering (där IT-säkerheten är en del) som harmonierar med SÄK:s rapportering. RIE utvecklar tydlig 2:a linjen-rapportering med infosäk som en del av den totala riskbilden	dec-22	IT-chef
9	SÄK, AID	Svårt fånga de kompetenser vi behöver om vi inte framstår som tillräckligt tydliga/attraktiva	Hög efterfrågan på cyberexpertis, svår marknad	AID, SÄK	4	4	H	Vara beredda att betala. Utforma tydliga och attraktiva roller. Behov av extern rekryteringshjälp/head hunting.	Vid rekr	Säk.chef, IT-chef, CISO
10	SÄK, RIE	Otydliga försvarslinjer på infosäk-området riskerar att skapa ineffektivitet	Bristande samsyn om försvarslinjer på säkerhetsskyddsområdet	Säkerhetschef, Riskchef	3	2	M	Se åtgärd risk 2	maj-22	Säk.chef, Riskchef
		Risker med nästa steg: att bevaka, analysera under uppstarten								
11		Svårt hitta en person som ska kunna axla ny tänkt säkerhetschefsroll, risk att rekrytering drar ut på tiden	Att axla rollerna Säkerhetschef+ Säkerhetsskydds-chef+ CISO-rapportering kommer att vara krävande, oavsett experter inom resp områden							

2.1 Övriga riskbedömningar från intressenter: Inga utöver de som angivits i tabellen.

2.2 Kommentarer från initiativet/projektet: På den workshop som genomfördes konstaterades att organisationsförändringen i sig framför allt var riskmitigerande – skapar bättre förutsättningar för tydliga roller och styrning.

3. Kvalitetssäkring RIE

Utförd av: Louise Bergström

Bedömning:

Riskenheten anser att riskerna beskrivs på ett tydligt sätt i mallen för riskanalys samt att relevanta enheter/funktioner har varit involverade samt informerade.

Riskenheten anser inte att den sammanvägda risknivån innebär något hinder att genomföra förändringen.

Rekommendationer:

Riskenheten rekommenderar att man analyserar eventuella intressekonflikter som skulle kunna uppstå p.g.a. denna organisatoriska flytt. Ett sådant exempel skulle kunna vara rapporteringslinjer och eventuella konflikter som uppstår p.g.a. förändringen. Om detta inte redan har diskuterats så anser riskenheten att det är bra att resonera kring detta och dokumentera slutsatser.