Beslutsunderlag

DATUM: 2022-04-12
AVDELNING: Stabsavdelningen
HANDLÄGGARE: Pether Burvall

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

Organisation av Riksbankens informationssäkerhet

Förslag till direktionens beslut

Direktionen beslutar att:

- ansvaret för styrningen av Riksbankens informationssäkerhet (den så kallade ”CISO-rollen”) flyttar från riskenheten på stabsavdelningen till säkerhetsenheten på avdelningen för verksamhetssupport,
- ändra i Instruktion för Sveriges riksbank enligt bilaga 1,
- stabsavdelningen och avdelningen för verksamhetssupport får i uppdrag att vidta de åtgärder som krävs för att detta ska kunna ske med verkan från 1 maj 2022,
- uppdra åt säkerhetsenheten att återkomma till direktionen med förslag till utveckling av styrningen av informationssäkerheten utifrån intentionerna i detta dokument, bl. a. i form av en cyberstrategi och reviderade styrdokument för informationssäkerhet.

Bakgrund

Cybersäkerhet prioriterat i den strategiska planen

Ett utvecklat skydd mot cyberhot är prioriterat i Riksbankens strategiska färdplan och en rad åtgärder pågår eller har redan vidtagits, som nytt ledningssystem för informationssäkerhet, en väsentlig utveckling för Riksbankens SOC (Security Operations Center), utvecklat säkerhetsskydd m.m. Beträffande *styrningen* av bankens

informationssäkerhet och cyberskydd har olika utmaningar och åtgärdsförslag diskuterats av Riksbankens externa rådgivare Gartner såväl som av interna sakkunniga.

Inriktningen enligt detta förslag har diskuterats internt och med den externa rådgivaren på området, Gartner, och resursplanerats i verksamhetsplanen för 2022. Ambitionen har varit att föreslå en tydligare organisation och styrning av informations-, IT och cybersäkerhet på Riksbanken med:

- En tydlig kravställning till utföraren, avdelningen för IT och Digitalisering (AID) med underleverantörer.
- Tydliga roller och mandat för första (säkerhetsenheten och AID) respektive andra (riskenheten) linjen.
- Förutsättningar för bra löpande status- och incidentrapportering till direktionen.
- En bedömning av vilka förmågor (kompetens och resurser) i egen bemanning eller i form av köpta tjänster som behöver tillföras olika funktioner, givet ovanstående.

Nuvarande organisation och styrning

Nuvarande organisation/roller på Riksbanken inom informations-, IT och cybersäkerhet (se informationssäkerhetspolicyn för formell beskrivning av nuvarande mandat):

- **Riskenheten (RIE), CISO**: Har ansvar för att leda, samordna arbetet och dokumentera mål, inriktning och krav för verksamhetens övergripande informations- och cybersäkerhet. Ansvaret innefattar även att stödja och följa upp att kraven är implementerade. Det ligger på CISO att lämna förslag till policy och regler samt att rapportera informationssäkerhetsläget för direktionen och ledningsgrupper. CISO är placerad på riskenheten, men har i praktiken blivit en mix av första och andra försvarslinjen.
- **Säkerhetsenheten (SÄK), säkerhetschef, säkerhetsskyddschef**: Har tidigare framför allt fokuserat på fysisk säkerhet, säkerhet för skyddsvärd verksamhet och personsäkerhet (t ex resesäkerhet). I takt med (1) hotutvecklingen, (2) att säkerhetsskyddslagen medfört högre krav och (3) att riskenheten strävat efter att skapa en tydligare roll, har man successivt lagt mer uppmärksamhet på informationssäkerhet – framför allt då för verksamhet som sorterar under säkerhetsskyddslagen. Utöver säkerhetschefen/ säkerhetsskyddschef har biträdande säkerhetschef en viktig roll.
- **Avdelningen för IT och digitalisering (AID)**: Ansvarar för IT-säkerheten, att med egna resurser och utkontrakterade tjänster hitta lösningar för att leva upp till kravbilden och successivt utveckla, anpassa och utvärdera det operativa skyddet. Viktiga roller här är IT-chef, chefen för enheten för arkitektur, IT-säkerhet och e-krona, IT-säkerhetsansvarig och SOC-ansvarig.
- **Avdelningen för finansiell stabilitet, enheten för finansiell infrastruktur (FSE)**: Ställer krav och rapporterar status för hur betalningssystemet RIX lever upp till de principer (PFMI, Principles for Financial Market Infrastructure) som Committee on Payments and Market Infrastructures (CPMI) fastställt för viktig finansiell

infrastruktur. EFS har även byggt förmågor för att övervaka cyberrisker i det finansiella systemet, där det främsta verktyget nu är TIBER-SE som under kontrollerade former simulerar cyberattacker mot finansiella institut. Härutöver pågår initiativ för att utveckla samverkansformerna mellan berörda myndigheter och finansiell sektor när det gäller cyberskydd.

- **Avdelningen för Betalningar, enheten för beredskap och samverkan (EBS)**: I takt med högre ambition för att klara av att driva samhällsviktig verksamhet vid höjd beredskap, ökar EBS:s roll som förmedlare av den kravbild som tas fram externt på området. Cyberresiliens innefattas i beredskapsarbetet och de flesta övningar och tester har inslag av cyberrelaterade risker.

Utmaningar med nuvarande organisation och styrning

Det finns ingen allmängiltig best practise för organisation och styrning av cybersäkerhet, det handlar för alla organisationer om att utifrån sina förutsättningar hitta tydliga roller som arbetar tillsammans mot tydliga mål – med respekt för vad de olika rollerna innebär. Riksbankens cyberskydd är väl utvecklat – banken har bra kompetens, har utvecklat och statusrapporterat mot ett nytt ledningssystem för informationssäkerhet (LIS) och på senare år utvecklat skyddet i rätt riktning och med hög ambition inom AID.

Det finns däremot perspektiv av *styrningen* som kan utvecklas successivt, till exempel:

- Den övergripande riskaptiten, målbilden, kravställningen och rapporteringsformerna behöver tydliggöras. Som framgår ovan finns flera olika kravställande funktioner för olika perspektiv av Riksbankens informationssäkerhet, inte minst för samhällsviktig verksamhet som RIX.
- Nuvarande CISO har att hantera en blandning av uppgifter som hör hemma i både första och andra försvarslinjen, och har som främsta verktyg att skriva styrdokument och ansvara för LIS, men saknar resurser (och egen budget) att styra arbetet i övrigt.
- Dessutom behövs fler dedikerade resurser med tydliga rollbeskrivningar. Resursökningar är beslutade i budget 2022, men det bör nämnas att arbetsmarknaden för att hitta den här typen av kompetens är utmanande.

Här fokuseras i första hand på hur vi kan organisera för att skapa en tydligare kravställning med fler dedikerade resurser – som i sin tur kan skapa tydligare mål, styrmodell och rapportering.

Extern kravbild för styrningen av informationssäkerhet

Det finns såväl nationella som internationella regler och vägledningar som Riksbanken, som ett minimikrav, ska uppfylla. Riksbanken ska självklart efterleva ambitionerna i tvingande lagstiftning och reglering, såsom säkerhetsskyddslagen, men ska även uppfylla CPMI:s vägledande principer för finansiell infrastruktur (PFMI). Vi ska också leva upp till principerna i MSB:s och SÄPO:s vägledningar för myndigheters arbete med informationssäkerhet. Därutöver har vi ambitionen att så långt som möjligt nå en nivå som kan anses vara best practise för centralbanker, svensk finansiell sektor och andra svenska myndigheter.

Tidigare riskanalyser, iakttagelser från internrevisionen och AFS/FSE:s granskning av RIX har dessutom resulterat i åtgärdsförslag som helt eller delvis anknyter till styrningen av informations-, IT- och cybersäkerhet.

Valet av styrmodell

Det vi har som en tydlig operativ styrmodell idag är LIS:en (som tar sin utgångspunkt i standarden ISO27000). Målsättningen är att nå en mognadsnivå fyra på en femgradig skala och att skapa mätbarhet i kontrollerna (utvärderingen är så här långt en självutvärdering av sakkunniga).

LIS kan sägas skapa ett strukturerat sätt att täcka helheten inom informationssäkerhets-arbetet. Det är ändå endast vad man kan betrakta som hygienfaktorer och vad som behöver vara på plats för att det ska finnas rätt *förutsättningar* för att den grundläggande informationssäkerheten ska fungera bra. Ambitionen är att utveckla det konceptet och göra LIS-utvärderingen mer mätbar och mindre beroende av kvalitativa bedömningar. Det stärker även trovärdigheten för LIS på lång sikt.

Men för att säkra att ett effektivt skydd måste vi utgå från tydliga utvärderingsbara mål och *löpande testa våra förmågor* att nå dem. Det som idag anges som direktionens mål i informationssäkerhetspolicyn – se ruta till höger – behöver ersättas med en målbild som tydligare uttrycker en mätbar risktolerans och mätbara mål.

En tydligare målbild ger förutsättningar för att skapa en gemensam syn på aktuell hotbild och aktuell status på vårt skydd mot den – genom löpande omvärldsanalys, tester och utvärderingar. Modellen ska så långt möjligt bygga på ”hårda” indikatorer som bankens olika funktioner ska uppnå tillsammans, med respekt för varandras olika roller.

Från Informationssäkerhetspolicyn (2020):

”Direktionens mål med Informationssäkerhet i Riksbanken är att tillämpa framstående standarder inom området, framförallt standarder som ISO27000, NIST CSF eller ISF Standard of Good Practice, samt att eftersträva en mognad i arbetet som är jämförbar eller bättre än andra centralbanker av samma storlek.”

Implementering av ramverket NIST Cyber Security Framework (NIST CSF) har diskuterats, inte minst för att det är en välrenommerad standard i arbetet med cybersäkerhet. NIST CSF bygger på fem förmågor (Identify, Protect, Detect, Respond, Recover) som genom tester mäts kontinuerligt och rapporteras mot hotbildsscenarion. Den nya kravställande organisationen bör bedöma hur det harmonierar med AID:s nuvarande kontrollkatalog och om/när det skulle vara rimligt att i så fall införa en sådan standard, med beaktande av att det skulle medföra fler kontroller och löpande uppföljningsaktiviteter.

Förslag till reviderad organisation

Ambitionen är alltså att skapa en tydlighet i roller och ansvar för informationssäkerheten på Riksbanken. Det betyder bland annat tydlighet i kravställning och uppföljning samt ett tydligt ansvar för genomförande av Riksbankens skydd mot informationssäkerhetsrisker. För att uppnå detta föreslås följande rollfördelning, vilket är i linje med rekommendationerna från direktionens externa rådgivare, Gartner:

1. **Renodla RIE:s organisatoriska ansvar för cyber:** Fortsätta renodla ansvaret utifrån ansvarslinjerna där RIE som andra linjen tar ansvar för att i samråd med 1:a linjen etablera risktoleransen för informationssäkerhetsrisker och följer upp på dessa i de befintliga processer som finns inom operationell riskhantering. Riksbankens informationssäkerhetsrisker får dela plats med övriga risker i RIE:s riskportfölj och blir därmed jämförd på lika villkor. Som ett led i att renodla rollen föreslås att nuvarande CISO-roll flyttas till första linjen. Det skapar en tydlig ansvarsfördelning av verksamhetsutvecklingen på området och förbättrar förutsättningarna för en oberoende riskuppföljning av Riksbankens cyberriskexponering och hur den svarar upp mot ställda krav och förväntningar från lagstiftning och samarbetsorganisationer.
2. **Utöka SÄK:s organisatoriska ansvar för kravställning av informationssäkerhet:** SÄK:s ansvar som kravställare föreslås utökas till att omfatta alla perspektiv på säkerhet för Riksbankens verksamhet, inklusive informationssäkerhetsarbetet. Som en naturlig del i ansvaret bör uppföljning på kravställning också finnas med genom förvaltning av LIS och statusrapportering till direktion och ledningsgrupp. Det skapar förutsättningar för en tydlig kravställning med ett helhetsperspektiv på säkerhet för hela Riksbankens verksamhet och för tydlig rapportering av efterlevnaden av ställda krav och av mognaden i cybersäkerhetsarbetet. SÄK blir dessutom den självklara kontaktpunkten för andra myndigheter och externa forum. Förslaget tar dessutom hänsyn till säkerhetsskyddschefens lagstadgade ansvar beträffande cybersäkerhet för samhällsviktig verksamhet.
3. **Förtydliga AID:s organisatoriska ansvar för leverans och uppföljning av IT- och cybersäkerhet:** Befästa AID:s ansvar att hitta lösningar för – och leverera på – uppsatta krav genom egna säkerhetsåtgärder och förvaltning och/eller genom kravställning och uppföljning av tredjepart.

Förslaget innebär alltså en mer samlad kravställning, i stort i enlighet med den externa rådgivaren Gartners förslag. På sikt, i samband med rekrytering av ny säkerhetschef (inför nuvarande chefs pensionsavgång) bör dessutom övervägas om rapporteringsmandatet för säkerhetschef, säkerhetsskyddschef och CISO bör samlas i en och samma befattning. Det vill säga *en* person som är direktionens kontaktpunkt för både cybersäkerhet och övriga perspektiv på säkerhet, som ansvarar för att föreslå mål respektive rapportera status.

Organisationen av funktioner i gränslandet till detta område, framför allt dataskydds- och beredskapsfrågor, har inte analyserats på djupet i detta arbete, men bör diskuteras längre fram.

Roller, förmågor och resurser som behövs i den nya organisationen

RIE i den nya organisationen

Informationsriskansvarig: med ansvar för att följa upp risker relaterade till informationssäkerhetsarbetet genom redan befintliga riskhanteringsprocesser. Stöd och support främst till säkerhetsorganisationen i bedömningen av säkerhetsrisker. Stöd och

support till verksamheten i RIE:s etablerade processer vid riskanalyser, beredningsärenden samt incidentrapportering. (Initialt 1 årsarbetare dedikerad)

SÄK i den nya organisationen

Eftersom säkerhetsenheten historiskt framför allt fokuserat på andra perspektiv av säkerhet (fysisk säkerhet och personsäkerhet) har man idag motsvarande en årsarbetare dedikerad till informationssäkerhet. För ett nytt SÄK är det rimligt att anta att det behöver organiseras i olika grupper för olika perspektiv – bl. a. en informationssäkerhetsansvarig som leder den grupp som kravställer informationssäkerhetsskyddet. (Initialt skapas i VP 2022 utrymme för 4 dedikerade exklusive säkerhetschef)

- *Säkerhetschef* (inkl. säkerhetsskyddschef och på sikt ev. CISO-mandat): Om beslut senare tas om att samla rollerna i en person kräver det kompetens i alla perspektiv (informations-, fysisk-, personsäkerhet och säkerhetsskydd) och en kommunikativ förmåga för att dels leda ledningen i diskussioner om hotbild och vad som är en rimlig skyddsnivå, dels rapportera status.
- *Informationssäkerhetsspecialister (3 st)*: med ansvar för att ställa krav och följa upp. Stöd och support för hela verksamheten med att analysera hot och risker samt ställa krav som främjar informationssäkerheten och verksamheternas arbete. Bidrar med medvetenhetshöjande och utbildande aktiviteter. En av specialisterna kan få ett uttalat ansvar som gruppchef för informationssäkerhet under säkerhetschefen.
- *LIS-specialist*: med ansvar för att driva LIS arbetet framåt och effektivisera efterlevnadskontrollerna. Utvecklar automation och strukturkapital samt rapportering.

AID i den nya organisationen

Som tidigare nämnts, ett oförändrat men förtydligat ansvar med fler dedikerade resurser med följande kompetens (initialt finns i VP 2022 utrymme att utöka med fyra dedikerade årsarbetare).

- *IT-säkerhetschef:* med ansvar för att leda och styra allt arbete med IT- och cybersäkerhet.
- *IT-säkerhetsansvarig*: med ansvar för att leda och samordna det operativa IT-säkerhetsarbetet samt dokumentera och rapportera utifrån uppsatta mål.
- *IT-säkerhetsarkitekter*: med ansvar för att med egna resurser eller utkontrakterade tjänster hitta lösningar för att leva upp till verksamhetens behov samt kravbilden avseende informationssäkerhet.
- *SOC-ansvarig:* med ansvar för att leda och styra SOC-arbetet.
- *Säkerhetsanalytiker*: med ansvar för analys av sårbarheter och risker inom infrastruktur och IT-förvaltning inom Riksbankens IT-stöd (inom ramen för Riksbankens SOC).

- *Penetrationstestare*: med ansvar för att genomföra/samordna säkerhetstester av Riksbankens IT-stöd.
- *Projektledare*: med ansvar för att driva verksamhetsplanerade aktiviteter för att utveckla skyddet.

Sammantaget skapades i Budget 2022 utrymme för en utökning med 6 nya tjänster för området – varav 4 på AID.

Riskanalys

MBL-process och riskanalys ur ett arbetsmiljöperspektiv har genomförts. Dessutom har en riskanalys utförts utifrån processen ”Beredning av väsentliga verksamhetsförändringar”. Bedömningen är att förändringen framför allt *hanterar* risker för en ineffektiv styrning, men det finns ändå risker som ska beaktas. Dessa redogörs för i bilaga 2, där riskanalysen dokumenteras. Viktigt inte minst att de medarbetare som har viktiga roller i den fortsatta uppbyggnaden av informations-/IT-/cybersäkerhet på Riksbanken kan samlas för ett par heldagsmöten, diskutera mål och utvecklingsplan och skapa en gemensam förståelse för hur olika roller ska bidra och samverka i uppbyggnaden. Den diskussionen behöver även omfatta eventuella intressekonflikter till följd av förändringen och landa i dokumenterade slutsatser för hur de i så fall ska hanteras – i enlighet med riskenhetens rekommendation (se bilaga 2).

Bilagor:

Bilaga 1: Bilaga till instruktionen, med ändringsmarkeringar

Bilaga 2: Riskanalys vid verksamhetsförändring