

Direktionens styrning av Riksbankens informationssäkerhet

2017-12-15

S V E R I G E S R I K S B A N K

Protokollsbilaga B
Fullmäktiges protokoll
2017-12-15, § 4b

Riksbankens dnr 2017-00177



Fullmäktiges
revisionsfunktion
Martin Malm,
Transcendent Group

Direktionens styrning av Riksbankens informationssäkerhet

Syfte

Syftet med granskningen är att bedöma att informationssäkerheten på Riksbanken är god genom direktionens styrning.

Risk att direktionen inte styr informationssäkerheten på ett lämpligt sätt. Detta kan leda till otydlighet samt oklara förväntningar och ansvar. I förlängningen leder det till ökad risk för brister inom informationssäkerheten.

Direktionens styrning av Riksbankens informationssäkerhet

Revisionsfunktionens referensram

- Lag (1988:1385) om Sveriges riksbank
- Arbetsordning
- Instruktion för Sveriges riksbank
- Policy för intern styrning och kontroll
- Regel för operativa risker
- Regel styrning av IT-säkerhet



Direktionens styrning av Riksbankens informationssäkerhet

Metod

Granskningen har utförts genom intervjuer och granskning av relevant dokumentation.

Dokumentation som inkluderats i granskningen är:

- Klassificering och hantering av Riksbankens information
- Riskrapportering till direktionen
- Dokument "förutsättningar för verksamhetsplan och budget 2018"
- Befattningsbeskrivning IT-säkerhetsansvarig
- Policy för intern styrning och kontroll
- Regel för operativa risker
- Regel styrning av IT-säkerhet

Intervjuer och avstämningar

- Thomas Lundin, Säkerhetschef
- Ulrika Pidestål, IT-chef
- Mithra Sundberg, Riskchef
- Simon Rörborn, Internrevisionschef
- Stefan Ingves, Riksbankschef
- Kerstin af Jochnick, Vice Riksbankschef

Direktionens styrning av Riksbankens informationssäkerhet

Övergripande bedömning

- Riksbankens direktion prioriterar arbetet med informationssäkerhet (IT-säkerhet/Cybersäkerhet)
- Erforderliga resurser tillförs den operativa verksamheten
- Direktionens delegering av ansvaret för informationssäkerhet är otydligt
- Riksbanken saknar ett Ledningssystem för informationssäkerhet

Direktionens styrning av Riksbankens informationssäkerhet

Iakttagelse

Revisionen bedömer utifrån granskningen att det finns brister i direktionens sätt att leda arbetet med informationssäkerhet på Riksbanken.

- Granskningen finner brister i det formella avseende styrning av informationssäkerheten på Riksbanken. Det saknas ett utpekat ansvar för detta område. Det saknas även ett ledningssystem för informationssäkerhet (LIS) där ett sådant ansvar skulle finnas utpekat.
- I praktiken är chefen för Riskenheten närmast att finna som ansvarig för informationssäkerheten. Men även säkerhetschefen ser sig som ansvarig för informationssäkerhet avseende de delar som faller under säkerhetsskydd, som vissa system gör. Inom IT finns även en utpekad resurs med ansvar för IT-säkerheten.

Direktionens styrning av Riksbankens informationssäkerhet

Rekommendation

- Riksbanksfullmäktiges granskningsfunktion rekommenderar att direktionen i sin styrning av informationssäkerheten på Riksbanken låter utreda och tydliggöra var ansvaret för detta viktiga område ska ligga.
- Vidare rekommenderar vi att direktionen låter utreda om Riksbanken ska efterleva Myndigheten för Samhällsskydd och Beredskaps föreskrifter om statliga myndigheters informationssäkerhet [2016:1] och därmed välja att införa ett Ledningssystem för informationssäkerhet (LIS).