Uppföljande granskning

Direktionens styrning av Riksbankens informationssäkerhet

2019-05-10

SVERIGES RIKSBANK

Protokollsbilaga A
Fullmäktiges protokoll
2019-05-10, § 4

Diarienummer 2019-00654

SVERIGES RIKSBANK

Fullmäktiges revisionsfunktion
Martin Malm,
Transcendent Group

Uppföljande granskning

Revisionsfunktionen har utfört en uppföljningsgranskning på den iakttagelse som noterades inom granskningen ”Styrning av informationssäkerhet”, daterad 2017-12-15:

- Revisionen bedömde då utifrån granskningen att det fanns 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

Uppföljande granskning
Direktionens styrning av Riksbankens informationssäkerhet

Syfte

Syftet med den uppföljande 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”
- Policy för informationssäkerhet
- Policy för intern styrning och kontroll
- Regel för operativa risker
- Regel styrning av IT-säkerhet

Intervjuer och avstämningar

- Thomas Lundin, Säkerhetschef
- Ulrika Pilestål, IT-chef
- Tomas Edlund tf riskchef
- Lars Andersson, Informationssäkerhetschef
- Simon Rörborn, Internrevisionschef
- Stefan Ingves, Riksbankschef
- Kerstin af Jochnick, Vice Riksbankschef

Resultat från uppföljningen (1)

Övergripande bedömning avseende utpekat ansvar

Sedan februari 2018 finns en utsedd informationssäkerhetschef på Riksbanken, Lars Andersson, som rapporterar till chefen för Riskenheten men även till Direktionen regelbundet.

Vi kan därmed konstatera att iakttagelsen avseende brister i utpekat ansvar är åtgärdad genom Direktionens delegering till en utsedd informationssäkerhetschef.

Resultat från uppföljningen (2)

Övergripande bedömning avseende införande av ledningssystem för informationssäkerhet (LIS)

Direktionen har genom beslutad policy för informationssäkerhet, beslutad 2108-05-22, bestämt att Riksbanken ska införa ett LIS. Arbetet med att införa detta har ålagts informationssäkerhetschefen. Arbetet har påbörjats under våren 2019. Rapportering avseende arbetet sker regelbundet till direktionen samt till styrgrupp för informationssäkerhetsarbetet på Riksbanken. Vidare bevakar internrevisionen löpande arbetet med införandet.

Vi kan därmed konstatera att iakttagelsen avseende utredning av och beslut om införande av LIS är åtgärdad.