NR 6 - december 2024

Revisionskontoret

Sammanfattning av granskningsrapport

Granskning av informations- och it-säkerhet inom nämnden för operativ regiongemensam verksamhet (NORV)

Uppdrag och syfte

Revisorerna har genomfört en granskning av informations- och it-säkerhet inom NORV. KPMG AB har biträtt i granskningsarbetet. Syftet med granskningen har varit att bedöma om NORV arbetar ändamålsenligt och effektivt med informationssäkerhet avseende Region Skånes it-system.

Resultat av granskningen

Den sammanfattande bedömningen är att NORV delvis arbetar ändamålsenligt och effektivt med informations- och it-säkerhet avseende Region Skånes it-system. I rapporten framgår att NORV inte beslutat om strategiska styrdokument som är relevanta för drift av verksamheten inom it. Det saknas en tydlig reglering avseende ansvarsfördelning mellan regionstyrelsen och NORV. Vidare visar granskningen att det inte finns en ändamålsenlig organisation med roller och ansvar för informationssäkerheten tydliggjord och uppfattad mellan Region Skånes olika verksamheter och Digitalisering och MT.

Regionstyrelsen rekommenderas att

- Bereda förslag till nytt reglemente för regionstyrelsen och NORV i syfte att tydligare reglera ansvaret för Region Skånes informationssäkerhetsarbete. Vid revideringen bör beaktas att det inom informationssäkerhetsområdet finns behov av att fatta beslut som påverkar andra nämnder i Region Skåne.
- Revidera riktlinjer och tillhörande instruktioner så att dessa är aktualiserade i enlighet med Region Skånes nuvarande organisation och ansvar samt kompletteras med reglering av ansvar för informationssäkerhetsarbetets olika delområden.
- Följa upp att de prioriterade åtgärder för utveckling av informationssäkerhetsarbetet som föreslogs i informationssäkerhetsberättelsen har en framdrift och stärker Region Skånes arbete.
- Överväga om vissa aktiviteter och uppgifter inom informationssäkerhetsarbetet kan integreras i den nya styr- och ansvarsmodellen.
- Stärka uppföljning och kontroll av efterlevnad av fastställda styrdokument inom informationssäkerhet.
- Säkerställa att en analys genomförs utifrån eventuellt nya krav med anledning av NIS2-direktivet samt att åtgärder vidtas i syfte att efterleva direktivet inom styrelsens ansvarsområden.

NORV rekommenderas att

- Bedöma om nuvarande styrning av förvaltningarnas arbete inom informationssäkerhet och tekniska säkerhetsåtgärder är tillräckliga utifrån nämndens ansvar, samt vid behov besluta om eller bereda förslag till kompletterande instruktioner och anvisningar.
- Säkerställa att informationssäkerhetssamordnare inom Digitalisering IT och MT har förutsättningar att utföra uppdraget i enlighet med det mandat som tillskrivs rollen.
- Tillse att förvaltningsledningen från informationssäkerhetssamordnaren erhåller en årlig samlad rapportering av informationssäkerhetsarbetet inom den egna förvaltningen i syfte att säkerställa en ändamålsenlig rapportering till nämnden.
- Säkerställa att den årliga uppföljningen inkluderar regelefterlevnad av lagkrav och styrande dokument inom informationssäkerhet och att brister rapporteras till nämnden samt till informationssäkerhetschef på koncernkontoret.
- Tillse att nuvarande uppföljning och rapportering till nämnden kompletteras med väsentliga händelser inom informationssäkerhet, exempelvis inträffade incidenter eller andra faktorer som riskerar att påverka nämndens ansvar inom drift av it.
- Säkerställa att en analys genomförs utifrån eventuellt nya krav med anledning av NIS2-direktivet samt att åtgärder vidtas i syfte att efterleva direktivet inom nämndens ansvarsområden.

Rapporten finns tillgänglig på www.skane.se/revisionen