Eva Tency Nilsson
Certifierad kommunal revisor
evatency.nilsson@skane.se

MISSIV
Datum 2024-12-17
Dnr 2024-RG000046

Regionstyrelsen
Nämnden för operativ regiongemensam verksamhet

Granskning av informations- och it-säkerhet inom nämnden för operativ regiongemensam verksamhet (NORV) - Rapport nr 6 – 2024

Den sammanfattande bedömningen är att nämnden för operativ regiongemensam verksamhet 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 i reglementen avseende ansvarsfördelning mellan regionstyrelsen och NORV. Detta utgör en risk för att det saknas en strategisk inritning för och styrning av arbetet med de tekniska skyddsåtgärderna i Region Skåne. Då den samlade kompetensen inom drift av it och tillhörande säkerhet finns inom NORVs verksamheter så är det väsentligt att nämnden vid behov bereder ärenden och underlag för beslut i regionstyrelsen, om behov av detta identifieras.

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 IT och MT. Det saknas tydlig rollbeskrivning både i reglementen och de regionövergripande styrdokumenten utifrån nuvarande organisation och hur arbetet genomförs i praktiken. I allt väsentligt finns erforderlig kompetens för ett ändamålsenligt arbete med informations- och it-säkerhet i förvaltningarna under NORV och att medarbetarna får kontinuerlig utbildning inom området. Dock görs bedömningen att det ur ett regionövergripande perspektiv behöver säkerställas att det finns en erforderlig kompetens genom ett aktivt utbildningsarbete av medarbetare i övriga förvaltningar och verksamheter.

Granskningen visar också att NORV i allt väsentligt säkerställer ett tillräcklig skydd för Region Skånes databaser och system inklusive molntjänster och att tekniska säkerhetsåtgärder vidtas utifrån de

identifierade skyddsvärden från informationsklassning och riskbedömning. Det poängteras dock att nämnden i låg grad är involverad i säkerställandet av skydd. Detta då varken information eller beslut om risker, åtgärder eller uppföljning i nuläget hanteras av NORV.

Det framgår också att NORV delvis säkerställt en ändamålsenlig incidenthantering och i allt väsentligt säkerställt en ändamålsenlig kontinuitetshantering. Bedömningen baseras på att det finns rutiner utifrån it-säkerhetsincidenter. Däremot bedöms att det är en brist att det saknas en fungerande incidenthantering för informationssäkerhetsincidenter, vilket är ett regionövergripande problem som även påverkar ändamålsenligheten i NORV:s förvaltningars incidenthantering.

I bilaga till detta missiv lämnar vi **rekommendationer** till regionstyrelsen och nämnden för operativ regiongemensam verksamhet. I bilaga anges också instruktioner för yttrande samt svarsformulär.

Revisorskollegiet behandlade rapporten vid sammanträdet 2024-12-17 och beslutade att översända missiv och rapport för yttrande till regionstyrelsen och nämnden för operativ regiongemensam verksamhet. Yttranden med uppgifter om verkställda och planerade åtgärder ska lämnas senast 2025-03-31.

För revisorskollegiet

Peter J Olsson
Ordförande

George Smidlund
Revisionsdirektör

Bilaga

Revisorernas rekommendationer

Rekommendationer till regionstyrelsen:

- 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.

Rekommendationer till nämnden för operativ regiongemensam verksamhet:

- 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.

Anvisningar för yttrande

- Svaret ska innehålla uppgifter om vilka åtgärder som vidtagits eller planeras vidtas utifrån revisorernas rekommendationer.
- Det ska finnas en tydlig koppling mellan de rekommendationer som revisorerna lämnat och de åtgärder som beskrivs i svaret.
- Svaret bör så långt det är möjligt innehålla tidsangivelser för när åtgärderna genomförs.
- Svaret bör så långt det är möjligt innehålla beskrivning hur åtgärderna genomförs.
- Svaret bör så långt det är möjligt beskriva vilken eller vilka funktioner inom förvaltningen eller sjukhuset som fått i uppdrag att arbeta med åtgärderna.
- Om styrelsen/nämnden inte planerar att vida några åtgärder, motivera varför.
- Om styrelsen/nämnden inte kan svara på utsatt tid, kontakta revisionskontoret.

Nedan bifogas formulär som kan användas för svar på revisorernas rekommendationer. Syftet med formuläret är att underlätta kommunikationen och därmed tydliggöra vilka åtgärder styrelsen och nämnden vidtagit eller planerar att vidta.

Svarsformulär för regionstyrelsen

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.
Regionstyrelsens svar:
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.
Regionstyrelsens svar:
Följa upp att de prioriterade åtgärder för utveckling av informationssäkerhetsarbetet som föreslogs i informationssäkerhetsberättelsen har en framdrift och stärker Region Skånes arbete.
Regionstyrelsens svar:
Överväga om vissa aktiviteter och uppgifter inom informationssäkerhetsarbetet kan integreras i den nya styr- och ansvarsmodellen.
Regionstyrelsens svar:
Stärka uppföljning och kontroll av efterlevnad av fastställda styrdokument inom informationssäkerhet.
Regionstyrelsens svar:
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.
Regionstyrelsens svar:
Övriga kommentarer:
Regionstyrelsens svar:

Svarsformulär för nämnden för operativ regiongemensam verksamhet:

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.
Nämndens svar:
Säkerställa att informationssäkerhetssamordnare inom Digitalisering IT och MT har förutsättningar att utföra uppdraget i enlighet med det mandat som tillskrivs rollen.
Nämndens svar:
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.
Nämndens svar:
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.
Nämndens svar:
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.
Nämndens svar:
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.
Nämndens svar:
Övriga kommentarer:
Nämndens svar: