NR 4 - Nov 2023

Revisionskontoret

Sammanfattning av granskningsrapport

Granskning av IT-säkerhet kollektivtrafiken

Uppdrag och syfte

Revisorerna har genomfört en granskning av IT-säkerheten inom kollektivtrafiken där KPMG AB har biträtt i granskningsarbetet.

Syftet med denna granskning har varit att bedöma om Region Skåne har säkerställt en tillräcklig IT-säkerhet inom Skånetrafikens IT-system.

Resultat av granskningen

Den samlade bedömningen är att kollektivtrafiknämnden inte har säkerställt att IT-säkerhetsarbetet är ändamålsenligt inom Skånetrafiken.

Region Skåne har ett ledningssystem för informationssäkerhet som inkluderar fastställda styrdokument i form av policys och riktlinjer för informationssäkerhetsarbetet som alla förvaltningar har att efterleva. Ledningssystemet för informationssäkerhet är inte etablerat i tillräcklig utsträckning inom Skånetrafiken vilket har genererat en bristfällig kännedom om gällande styrdokument och krav. Det saknas därigenom etablerade processer och aktiviteter för IT-säkerhetsarbetet i enlighet med den struktur och systematik som arbetet ska bedrivas inom. Den ansvarsfördelning som är dokumenterad omsätts inte i praktiken och roller avseende IT-säkerheten för de system som nyttjas inom kollektivtrafiken är inte tydligt definierad.

Rekommendationer till regionstyrelsen:

- Revidera styrdokument så att dessa är aktuella och utgör en ändamålsenlig styrning av informationssäkerhetsarbetet i Region Skåne.
- Säkerställa att ledningssystemet för informationssäkerhet etableras i samtliga verksamheter och att aktiviteter genomförs i enlighet med den systematik som beslutats.
- Utvärdera om organisation och funktioner är anpassade i förhållande till ledningssystemets omfattning och krav på hur informationssäkerhetsarbetet ska bedrivas.
- Säkerställa att regionstyrelsen i sin uppsiktsplikt stärker den interna kontrollen över efterlevnad av styrande dokument.

Rekommendationer till kollektivtrafiknämnden:

- Säkerställa att informationssäkerhetsarbetet genomförs i enlighet med beslutade krav och systematik.
- Säkerställa att roll- och ansvarsfördelning tydliggörs och etableras inom kollektivtrafiknämndens verksamheter.
- Säkerställa att kontinuitetsplaner för störning och avbrott upprättas för IT-system inom kollektivtrafiknämnden samt att övning och granskning genomförs i syfte att säkerställa ändamålsenlighet, aktualitet och kunskap.
- Säkerställa att informationsklassning och riskanalyser genomförs systematiskt på de informationstillgångar som hanteras i verksamheten samt att åtgärdsplaner upprättas utifrån erhållet resultat.
- Säkerställa att säkerhetsåtgärder vidtas i syfte att skydda informationstillgångar och för att minimera eller eliminera risker som identifierats samt att dessa utvärderas regelbundet.
- Säkerställa att gällande incidenthanteringsrutiner etableras samt att inträffade incidenter utgör del i uppföljning och förbättringsarbete så att väsentliga brister kan identifieras och åtgärdas.
- Säkerställa att den uppföljning som sker av informationssäkerhetsarbetet även inkluderar IT-säkerhet.
- Stärka den interna kontrollen avseende efterlevnad av styrdokument för informationssäkerhet.
- Säkerställa att nämnden erhåller återrapportering i tillräcklig utsträckning i syfte att kunna fatta beslut om erforderliga åtgärder för att stärka IT-säkerheten.

Rapporten finns tillgänglig på www.skane.se/revisionen