Helén Löwgren
Helen.Lowgren@skane.se

YTTRANDE

Datum 2025-02-28
Ärendenummer 2024-POL000486

Yttrande Granskningsrapport Granskning av informations- och it-säkerhet inom nämnden för operativ regiongemensam verksamhet (NORV) rapport nr 6 2024 Regionstyrelsen

Region Skånes revisorer har genomfört en granskning av arbetet med informations- och it-säkerhet inom nämnden för operativ regiongemensam verksamhet. 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. Bedömningen är även att det saknas en tydlig reglering i reglementen avseende ansvarsfördelning mellan regionstyrelsen och NORV.

Regionstyrelsen önskar framföra följande synpunkter på revisionens rekommendationer.

***Rekommendation:* 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 bedömning är att arbetet med informationssäkerhet omfattas av regionens ”Policy för säkerhet och beredskap” (fastställd av regionfullmäktige 2024-12-03) och ”Riktlinje för informationssäkerhet” (fastställd av Regionstyrelsen 2017-12-07). I dokumentet ”Instruktion för tillämpning av riktlinje för informationssäkerhet” anges därutöver organisation, roller och ansvar kopplat till arbetet med informationssäkerhetsarbetet i Region Skåne.

För närvarande pågår en revidering av ”Riktlinje för informationssäkerhet” där övergripande ansvar och roller inom informationssäkerhetsarbetet kommer att förtydligas ytterligare. De reviderade riktlinjerna ska upp till beslut i regionstyrelsen under våren 2025.

Rekommendation: **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.**
Regionstyrelsen instämmer i att riktlinjer och tillhörande instruktioner inte kontinuerligt har uppdaterats, men regionstyrelsen instämmer inte i att riktlinjen saknar reglering av ansvar för informationssäkerhetsarbetet.

I den tidigare nämnda revideringen av ”Riktlinje för informationssäkerhet” föreslås informationssäkerhetschefen/enhetschefen få beslutanderätt över regionövergripande instruktioner och anvisningar inom informationssäkerhetsområdet (vilket regiondirektören ansvarar för idag). Då kommer tillhörande instruktioner och anvisningar kunna revideras mer frekvent, än under nu gällande ansvarsfördelning. De reviderade riktlinjerna ska upp till beslut i regionstyrelsen under våren 2025 och övriga instruktioner och anvisningar är analyserade och prioriterade av Enheten för Informationssäkerhet och Dataskydd på Koncernkontoret inför en revideringsuppstart som kommer påbörjas under 2025. Framöver kommer kontinuerligt revisioner att göras utefter behov.

Rekommendation: **Följa upp att de prioriterade åtgärder för utveckling av informationssäkerhetsarbetet som föreslogs i informationssäkerhetsberättelsen har en framdrift och stärker Region Skånes arbete.**
Från och med i år kommer Informationssäkerhetsorganisationen arbeta med kortsiktiga mål på ett annat sätt än tidigare, den regionala enheten kommer nu tillsammans med nämndernas olika förvaltningars samordnare välja ut 3 prioriterade områden där mognaden är låg, enligt förra årets mognadsmätning. Detta kommer ske på den inplanerade Informationssäkerhetsrådet den 10 mars. Förvaltningarna kommer tillsammans ta fram åtgärder (som kommer återfinnas i årets informationssäkerhetsberättelse), som sedan beslutas av regionstyrelsen i samband med årsrapporten. Dessa definierade åtgärder kommer förvaltningarna systematiskt arbeta med tillsammans under 2025–2026 och under denna tid kommer framdrift och effekt av åtgärderna frekvent följas upp och rapporteras.

Rekommendation: **Överväga om vissa aktiviteter och uppgifter inom informationssäkerhetsarbetet kan integreras i den nya styr- och ansvarsmodellen.**
För att lyckas med digitalisering måste information vara i centrum, regionstyrelsen kan se att en aktivitet som informationsklassning där informationens värde analyseras, det vill säga klassas, för att få ett skyddsvärde (ett KRT-värde) som representerar den nivå av skydd informationen behöver för att bevara sitt värde, kan vara en sådan aktivitet.

Klassningsprocessen för informationssäkerhet behöver ses över, detta arbete ska påbörjas under 2025, en första åtgärd är att definiera och fastställa K-värde för

alla informationsobjekt som informationsägarna äger och att dessa publiceras i en vägledning. Initialt kommer detta gälla hälso-sjukvårdsdirektörens, HR-direktörens, ekonomidirektörens och IT-direktörens informationsobjekt. Denna åtgärd uppskattas vara klar under 2026, och kommer utföras av Enheten för Informationssäkerhet och Dataskydd på Koncernkontoret.

Om man vet hur informationens ska skyddas vet man också hur informationen får hanteras och då blir det lättare att planera för digitaliseringsinsatser och därmed uppfylla politiska beslut om digital transformering.

***Rekommendation:* Stärka uppföljning och kontroll av efterlevnad av fastställda styrdokument inom informationssäkerhet.**
Ett samarbete har påbörjats redan vintern 2024 mellan Enheten för Informationssäkerhet och Dataskydd på Koncernkontoret och Enheten IT-säkerhet på DigIT/MT att ta fram kontroller för att kunna mäta efterlevnaden, detta är ett led i det gemensamma arbetet med införande av NIS-direktivet och kommande nationell lagstiftning som kommer pågå aktivt under 2025 för att sedan bli en del av det systematiska arbetet.

Enheten för Informationssäkerhet och Dataskydd på Koncernkontoret har även tagit fram ett utkast till en instruktion vars syfte är att styra och vägleda medarbetare i arbetet med revision och granskning av informationssäkerhet, baserat på DigIT/MT redan gällande instruktion. Arbetet med uppföljning och efterlevnad på ett mer systematiskt sätt kommer tidigast kunna påbörjas 2026. Initialt fokuserar den regionala enheten för informationssäkerhet på kontroll och efterlevnad av styrdokument kopplande till NIS-krav, en GAP-analys är genomför och under våren 2025 kommer mognadsmätningar göras.

***Rekommendation:* 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.**
Arbetet drivs av Enheten för Informationssäkerhet och Dataskydd på Koncernkontoret tillsammans med IT-säkerhetsenheten på DigIT/MT. Ett analysarbete påbörjades redan vintern 2024 och fem delleveranser, med åtgärder som ska vidtas, är identifierade och dokumenterade.

En GAP-analys är gjord under vintern 2024 på vilka säkerhetskrav som finns i Regions Skånes styrande dokument för informationssäkerhet. Under Q1 2025 har ett mognadsmätningsverktyg tagits fram, med hjälp av mognadsanalysen framgår fram hur väl (med vilken effekt) riktlinjerna efterlevs samt en lista på åtgärder som måste införas för att efterleva kraven i NIS-direktivet.

Uppdatering av riskhanteringsprocessen och incidentprocessen pågår och under våren 2025 kommer IT-stöd för riskanalyser börja användas som gör att med riskanalysarbetet kan ske mer systematiskt och effektivt. En ny process för incidenthantering har tagits fram under vintern 2024-2025 och som just nu håller på att införas.

Arbete som ännu inte påbörjats, men som är planerade, är planer för verksamhetskontinuitet, utbildning för ledningen och åtgärder för säkerhet i digitala leverantörskedjor. Dessa kommer påbörjas senast under andra hälften av 2025. Införandet av NIS-direktivet kommer fortgå under hela 2025 för att sedan bli en del av det systematiska förbättringsarbetet.

Carl Johan Sonesson
Ordförande

Lars-Åke Rudin
Regiondirektör