Dnr:RS/2381/2016

Anna-Lena Alfreds
Enheten för krisberedskap, säkerhet och miljö
Tfn: 063-147612
E-post: anna-lena.alfreds@regionjh.se

Svar på granskning av IT- och informationssäkerheten

Revisorerna för Region Jämtland Härjedalen har genom sitt revisionskontor genomfört en förstudie med syfte att kartlägga och bedöma om det finns anledning att besluta om en fördjupad granskning om hur informationssäkerhetsarbetet organiserats och bedrivs. Förstudien visar att det pågår ett aktivt arbete mot målet att säkerställa informations-säkerheten. Det finns dock en mängd kända brister av varierande allvarlighetsgrad. Åtgärder vidtas löpande men inte i tillräcklig takt. Det finns några mycket angelägna förbättringsområden som styrelsen rekommenderas att särskilt bevaka.

Nedan redovisas regionstyrelsens svar avseende vilka åtgärder den avser vidta med anledning av revisorernas rekommendationer samt när bakomliggande problem kan vara lösta.

Revisionsfråga

Sker arbetet med informationssäkerhet med en systematik som ger förutsättningar för att en tillräcklig säkerhet uppnås?

Revisorernas bedömning

Nej, inte ännu. Utveckling av systematik för informationssäkerhetsarbetet pågår, men det saknas ännu viktiga åtgärder inom en del områden. Det finns, vilket vi återkommer till i rapporten, stora brister i arbetet med klassning av informationen, problem med den systemförvaltningsmodell som tillämpas och kunskaper hos användarna.

Regionstyrelsens svar

Det finns en övergripande handlingsplan för informationssäkerhet som bl.a. innehåller mål och aktiviteter i syfte att etablera ett systematiskt och strukturerat arbetssätt för området.

Sedan ett år tillbaka är informationssäkerhet (enligt standarden ISO 27001) en del i ledningens genomgång vilket är regionens verktyg för att följa upp ledningssystemets funktionalitet. Det innebär också att riskanalyser, avvikelser/brister och förbättringsområden lyfts upp i både ledningsgruppen för hälso- och sjukvårdsförvaltningen, regionala utvecklingsförvaltningen och i regionledningen två gånger per år. Detta är en viktig del för att arbetet med informationssäkerhet ska kunna ske systematiskt. Vidare har regionstaben prioriterat att rekrytera en informationssäkerhetssamordnare som påbörjat sin tjänst under mars 2017. Det bedöms ge avsevärt bättre möjlighet till systematiskt uppföljnings- och utvecklingsarbete inom områden som tidigare har uppvisat brister. Det ger också bättre möjlighet att uppnå de mål och genomföra de aktiviteter som återfinns i handlingsplanen. Ett stöd i det kommande arbetet är också att en övergripande riskanalys för organisationens informationssäkerhet påbörjats. Analysen syftar till att identifiera de större risker som har framkommit i egen rapportering och omvärldsbevakning.

Revisionsfråga

Sker en planering och uppföljning av att standarden ISO 27001, så långt som möjligt, följs?

Revisorernas bedömning

Ja, ett arbete har påbörjats. En GAP-analys har gjorts och utveckling av formerna för uppföljning pågår. Med detta inte sagt att den nämnda standarden uppfylls.

Regionstyrelsens svar

Det finns inget enkelt sätt att mäta efterlevnad av ISO27001-standarden idag, men arbetet kommer att fortsätta för att utveckla formen för detta. Uppföljning behöver ske kontinuerligt, vilket bland annat görs som tidigare beskrivits genom internrevisioner och ledningens genomgång. I enlighet med revisorernas förslag ska arbete göras för att bättre tolka standardens krav och tydliggöra vilka krav som ska uppfyllas samt vilka krav som inte är lika prioriterade för regionen.

Revisionsfråga

Finns en tillräcklig kontroll över att inventeringen av säkerhetsproblem sker på ett ändamålsenligt sätt?

Revisorernas bedömning

Nej, inte fullt ut. Det finns brister i klassningen av informationen och i systemägarnas förutsättningar att klara sin roll och att uppfylla det ansvar den innefattar.

Regionstyrelsens svar

Under 2017 kommer en medarbetarutbildning i informationssäkerhet att tas fram. Det bedöms kunna ge förbättringar i säkerhetsmedvetande och gemensamma förhållningssätt för hur man ska agera, både förebyggande och när incidenter inträffar.

För att förbättra och stärka arbetet med systemförvaltning, informationsklassning och relaterade säkerhetsproblem planerar Region Jämtland Härjedalen att under 2017 byta metod och verktyg från BITS till KLASSA 2.0 som lanserats av Sveriges kommuner och landsting (SKL).

KLASSA bedöms vara enklare för systemägare och systemansvariga att använda. Det är också modernare och verktyget förvaltas och utvecklas av en styrgrupp i SKL. En ytterligare åtgärd som planeras för att förbättra förutsättningarna inom systemförvaltning är att redan under hösten 2017

starta upp ett forum för systemägare där kunskapsutbyte kan ske samt stöd erhållas avseende systemförvaltning. Fokus kommer till en början att ligga på det prioriterade området informationsklassning. Informationssäkerhetssamordnaren har tilldelats uppdraget som prioriterad uppgift. Det kommer också att ske en tydligare kravställning på systemägare att informationsklassning ska genomföras**.**

Gällande systemförvaltningsmodell tilldelades IT chefen ett uppdrag för göra en översyn av denna under 2016. I det arbetet skulle också de risker, brister samt förbättringsförslag som framkommit i tidigare genomförd riskanalys beaktas. Översynen kunde dock inte genomföras som planerat p.g.a. många vakanser inom IT- och ehälsoavdelningen samt IT chefens uppdrag under hösten 2016 att vara delprojektledare för regionbildning på 50%. IT chefen konstaterar att Pm3 modellen har många fördelar genom en samverkande förvaltningsorganisation, med IT respektive verksamhetskompetens. Samtidigt är modellen betydligt mer resurskrävande för både verksamhet och IT- och eHälsa än nuvarande modell. Mot bakgrund av de bemanningsproblem både inom vård och IT samt den ekonomiskt svåra situation som regionen befinner sig i, är det därför svårt att motivera denna ambitionsökning i dagsläget. En översyn av förvaltningsmodell kommer dock att prioriteras när förutsättningarna har förbättrats.

Revisionsfråga

Har det säkerställts att prioriterade åtgärder vidtas?

Revisorernas bedömning

Nej, det har vidtagits en rad positiva åtgärder men vi anser inte att det ännu är säkerställt att prioriterade åtgärder kommer att vidtas. Huvudsakligen beror detta på att informationsklassning inte är genomförd i tillräcklig utsträckning och därmed kan det finnas ett mörkertal av viktiga

åtgärders som borde lyfts upp för prioritering och att det saknas tydligt budget för att vidta åtgärder.

Regionstyrelsens svar

Den viktigaste åtgärden som vidtagits för att säkerställa att prioriterade åtgärder vidtas är att, som tidigare nämnts, en informationssäkerhetssamordnare anställts. Den resursen med rätt kompetens är avgörande för att prioriterade åtgärder ska kunna genomföras. Området behöver också fortsatt styras genom handlingsplaner och uppföljningar. För att arbeta så effektivt som möjligt med de resurser som finns i Region Jämtland Härjedalen är ett arbete nu påbörjat med att tydliggöra roller, ansvar och organisation inom informations- och IT säkerhetsfrågor. Gällande avsaknad av budget för informationssäkerhet har det lyfts fram i regionstabens arbete med ofinansierade behov. Dialog pågår för att skapa budgeterade resurser för arbete och anpassning för att möta kraven i den nya dataskyddsförordningen som börjar gälla 2018.

REGIONSTYRELSEN

Ann-Marie Johansson
Regionstyrelsens ordförande

Ingela Jönsson
Tf regiondirektör